ỦY BAN NHÂN DÂN TỈNH BÌNH DƯƠNG
TRƯỜNG CAO ĐẲNG NGHỀ VIỆT NAM - SINGAPORE

GIÁO TRÌNH

Mô đun: AN TOÀN MẠNG

NGHỀ:QUẢN TRỊ MẠNG MÁY TÍNH

TRÌNH ĐỘ TRUNG CẤP NGHỀ

Ban hành kèm theo Quyết định số: /QĐ-TCĐNVS ngày tháng năm của Trường Cao đẳng nghề Việt Nam - Singapore

Bình Dương, năm 2017

LỜI GIỚI THIỆU

Qua thời gian giảng dạy tại trường Cao Đẳng nghề Việt Nam-Singapore cùng với các Thầy Cô trong Khoa Công nghệ thông tin, bản thân tôi thấy cần biên soạn một tập tài liệu về ***An toàn mạng*** nhằm đáp ứng với chương trình giảng dạy hệ Cao Đẳng nghề quản trị mạng máy tính. Nội dung của giáo trình được tham khảo và biên soạn theo tài liệu quản trị mạng máy tính của Microsoft và giáo trình quản trị mạng của Đại học khoa học tự nhiên thành phố Hồ Chí Minh. Tập tài liệu trình bày về lý thuyết và các bước thực hành quản trị mạng máy tính, các giao thức truyền thông và các ứng dụng bao gồm những kiến thức cơ bản về các loại mạng, mô hình mạng, kiến trúc mạng, và các thiết bị kết nối mạng, mô hình OSI,TCP/IP … Với mong muốn tìm hiểu kỹ về công nghệ thông tin, mạng máy tính để có thể xây dựng, ứng dụng tối đa các tiện ích mà mạng máy tính mang lại sau khi học ***An toàn mạng***. Trong quá trình biên soạn tập tài liệu này dù đã cố gắng nhiều nhưng không thể tránh được những thiếu sót. Rất mong được sự góp ý của quí Thầy Cô để tập tài liệu này được hoàn chỉnh hơn.

Giáo trình này được biên soạn lại từ những nguồn tài liệu tham khảo khác nhau cho phù hợp với điều kiện giảng dạy tại Trường Cao đẳng nghề Việt Nam-Singapore và chỉ lưu hành nội bộ

Bình Dương, *ngày 31 tháng 12 năm 2018*

NGUYỄN ANH TUẤN-Tác giả

MỤC LỤC

MỤC LỤC 3
GIÁO TRÌNH MÔ ĐUN 6
BÀI 1:TỔNG QUAN VỀ BẢO MẬT VÀ AN TOÀN MẠNG 8
1. Các khái niệm chung 8
2. Nhu cầu bảo vệ thông tin 9
2.1 Sự cần thiết của an toàn thông tin 9
2.2.Mục đích của an toàn thông tin 9
2.3.Các nguy cơ mất an toàn thông tin 10
2.4.Các giải pháp bảo vệ an toàn thông tin 10
3. TÓM TẮT NỘI DUNG 11
4. CÂU HỎI 11
BÀI 2: MÃ HÓA THÔNG TIN 12
1. Căn bản về mã hoá 12
1.1.Tại sao cần phải mã hoá 12
1.2.Nhu cầu sử dụng kỹ thuật mã hoá 12
1.3.Quá trình mã hoá 12
2. Độ an toàn của thuật toán 14
3. Phân loại các thuật toán mã hoá 14
3.1 Mã hoá cổ điển 15
3.2 Mã hoá đối xứng 15
3.3 Mã hoá bất đối xứng 16
3.4 Hệ thống mã hoá khoá lai (Hybrid Cryptosystems) 17
4. Bài tập thực hành 18
5. TÓM TẮT NỘI DUNG 34
6. CÂU HỎI VÀ BÀI TẬP 34
BÀI 3: NETWORK ADDRESS TRANSLATION 40
1. Giới thiệu 40
2. Các kỹ thuật Nat cổ điển 40
2.1 NAT tĩnh 40
2.2 NAT động 40
3. NAT trong Windows server 40
4.Bài tập thực hành 41
5- TÓM TẮT NỘI DUNG 49
6- CÂU HỎI VÀ BÀI TẬP 50
BÀI 4 :BẢO VỆ MẠNG BẰNG TƯỜNG LỬA 54
1. Các kiểu tấn công 54
1.1.Tấn công trực tiếp 54
1.2. Nghe trộm 54
1.3. Giả mạo địa chỉ 54
1.4. Vô hiệu hoá các chức năng của hệ thống 54
1.5. Lỗi của người quản trị hệ thống 55
1.6. Tấn công vào yếu tố con người 56

2. Các mức bảo vệ an toàn 56
3. Internet Firewall 57
3.1 Định nghĩa 57
3.2 Chức năng 57
3.3 Cấu trúc 58
3.4. Các thành phần của Firewall và cơ chế hoạt động 59
3.4.1. Bộ lọc Paket (Paket filtering router) 59
3.4.2. Cổng ứng dụng (Application- Level Getway) 60
3.5. Những hạn chế của Firewall 61
3.6. Các ví dụ về Firewall 62
3.6.1. Packet- Filtering router (Bộ trung chuyển có lọc gói) 62
3.6.2. Screened host firewall 62
3.6.3. Demilitarized Zone (DMZ – khu vực phi quân sự) 63
4. Bài tập thực hành 64
5. TÓM TẮT NỘI DUNG 71
6. CÂU HỎI VÀ BÀI TẬP 71
BÀI 5: DANH SÁCH ĐIỀU KHIỂN TRUY CẬP 74
1. Khái niệm về danh sách truy cập 74
1.1 Giới thiệu về điều khiển truy cập 74
1.2 Các kiểu xác thực 74
1.3 Các nguy cơ và các điểm yếu của điều khiển truy cập 74
1.4 Một số ứng tiêu biểu của điều khiển truy cập 75
2. Nguyên tắc hoạt động của danh sách truy cập 75
2.1 Điều khiển truy cập tùy quyền (DAC - Discretionary Access Control) ... 75
2.2 Các giải pháp đảm bảo an ninh, an toàn dựa trên điều khiển truy cập 77
3. Bài tập thực hành 78
4- TÓM TẮT NỘI DUNG 86
5- CÂU HỎI VÀ BÀI TẬP 86
BÀI 6 :VIRUS VÀ CÁCH PHÒNG CHỐNG 90
1. Giới thiệu tổng quan về virus 90
1.1.Virus là gì ? 90
1.2 Các khái niệm có liên quan 90
2. Cách thức lây lan và phân loại virus 90
2.1 B-Virus 90
2.2 F-virus 91
3. Ngăn chặn sự xâm nhập virus 92
3.1 Sử dụng phần mềm diệt virus 92
3.2 Sử dụng tường lửa 93
3.3 Cập nhật các bản sửa lỗi của hệ điều hành 93
3.4 Vận dụng kinh nghiệm sử dụng máy tính 93
3.5 Bảo vệ dữ liệu máy tính 93
3.6 Sao lưu dữ liệu theo chu kỳ 93
3.7 Tạo các dữ liệu phục hồi cho toàn hệ thống 93
4- Bài tập thực hành 94

5-TÓM TẮT NỘI DUNG 100
6- CÂU HỎI VÀ BÀI TẬP 100
CÁC THUẬT NGỮ CHUYÊN MÔN 107
TÀI LIỆU THAM KHẢO 109

GIÁO TRÌNH MÔ ĐUN

Tên mô đun: AN TOÀN MẠNG

Mã số mô đun: MĐ 26

Thời gian thực hiện mô đun: 45 giờ; (Lý thuyết:15 giờ; Thực hành, thí nghiệm, thảo luận, bài tập: 27 giờ; Kiểm tra: 3 giờ)

I. Vị trí, tính chất của mô đun:

- Vị trí: Mô đun được bố trí sau khi sinh viên học xong các môn học chung, các môn cơ sở chuyên ngành đào tạo chuyên môn nghề bắt buộc.
- Tính chất: Là mô đun chuyên nghành bắt buộc.

II. Mục tiêu mô đun:

- Về kiến thức:
  + Xác định được các thành phần cần bảo mật cho một hệ thống mạng;
  + Trình bày được các hình thức tấn công vào hệ thống mạng;
  + Xác định được cách thức mã hoá thông tin;
  + Trình bày được quá trình NAT trong hệ thống mạng;
  + Xác định được khái niệm về danh sách truy cập;
  + Nêu được nguyên tắc hoạt động của danh sách truy cập;
- Về kỹ năng:
  + Thiết lập được các cách thức bảo mật
  + Cấu hình và xây dựng được các chính sách bảo mật
  + Thiết lập tường lửa bảo vệ mạng
  + Cài đặt được các phần mềm chống virus và thiết lập cấu hình các phần mềm đó
  + Phân biệt được các loại virus thông dụng và cách phòng chống virus.
- Về năng lực tự chủ và trách nhiệm: Bố trí làm việc khoa học đảm bảo an toàn cho người và phương tiện học tập

III. Nội dung mô đun:

SỐ TT	Tên các bài trong mô đun	Thời gian (giờ)			
		Tổng số	Lý thuyết	Thực hành, thảo luận, bài tập	Kiểm tra
1	**Bài 1:**Tổng quan về bảo mật và an toàn mạng	3	3	0	
2	**Bài 2:**Mã hóa thông tin	7	3	4	
3	**Bài 3:**NAT	8	2	5	1
4	**Bài 4:**Bảo vệ mạng bằng tường lửa	8	3	4	1
5	**Bài 5:**Danh sách điều khiển truy cập	14	3	10	1
6	**Bài 6:**Virus và cách phòng chống	5	1	4	
	Cộng	**45**	**15**	**27**	**3**

BÀI 1:TỔNG QUAN VỀ BẢO MẬT VÀ AN TOÀN MẠNG

Mã bài MĐ 26-01

Thời gian: 3 giờ

I. MỤC TIÊU: Sau khi học bài học này, sinh viên có khả năng

- Trình bày được khái niệm về an toàn thông và bảo mật thông tin
- Trình bày được nhu cầu và các giải pháp bảo mật thông tin
- Xác định được các thành phần của một hệ thống bảo mật
- Thực hiện các thao tác an toàn với máy tính

II. NỘI DUNG CHÍNH

1. Các khái niệm chung

An toàn thông tin: là các hoạt động bảo vệ tài sản thông tin và là một lĩnh vực rộng lớn. Nó bao gồm cả những sản phẩm và những quy trình nhằm ngăn chặn truy cập trái phép, hiệu chỉnh, xóa thông tin,... An toàn thông tin liên quan đến hai khía cạnh đó là an toàn về mặt vật lý và an toàn về mặt kỹ thuật.

Bảo mật thông tin: là bảo vệ thông tin dữ liệu cá nhân, tổ chức nhằm tránh khỏi sự "đánh cắp" bởi những kẻ xấu hoặc tin tặc. An ninh thông tin cũng như sự bảo mật an toàn thông tin nói chung. Việc bảo mật tốt những dữ liệu và thông tin sẽ tránh những rủi ro không đáng có cho chính cá nhân và tổ chức.

Bảo mật thông tin là duy trì tính bảo mật, tính toàn vẹn toàn diện và tính sẵn sàng cho toàn bộ thông tin. Ba yếu tố không thể tách rời trong việc bảo mật thông tin là:

Tính bí mật (Confidentiality): bảo vệ dữ liệu không bị lộ ra ngoài một cách trái phép. Ví dụ: Trong hệ thống ngân hàng, một khách hàng được phép xem thông tin số dư tài khoản của mình nhưng không được phép xem thông tin của khách hàng khác

Tính toàn vẹn (Integrity): Chỉ những người dùng được ủy quyền mới được phép chỉnh sửa dữ liệu. Ví dụ: Trong hệ thống ngân hàng, không cho phép khách hàng tự thay đổi thông tin số dư của tài khoản của mình.

Tính sẵn sàng (Availability): Đảm bảo dữ liệu luôn sẵn sàng khi những người dùng hoặc ứng dụng được ủy quyền yêu cầu. Ví dụ: Trong hệ thống ngân hàng, cần đảm bảo rằng khách hàng có thể truy vấn thông tin số dư tài khoản bất kỳ lúc nào theo như quy định

An ninh mạng máy tính (network security) là tổng thể các giải pháp về mặt tổ chức và kỹ thuật nhằm ngăn cản mọi nguy cơ tổn hại đến mạng.

Các tổn hại có thể xảy ra do:

+ Lỗi của người sử dụng,

+ Các lỗ hổng trong các hệ điều hành cũng như các chương trình ứng dụng,
+ Các hành động hiểm độc,
+ Các lỗi phần cứng,
+ Các nguyên nhân khác từ tự nhiên

2. Nhu cầu bảo vệ thông tin

Mục tiêu: trình bày được nhu cầu và các giải pháp bảo mật thông tin

Ngày nay với sự phát triển bùng nổ của công nghệ thông tin, hầu hết các thông tin của các tổ chức, cá nhân đều được lưu trữ trên hệ thống máy tính. Cùng với sự phát triển của tổ chức là những đòi hỏi ngày càng cao của môi trường hoạt động cần phải chia sẻ thông tin của mình cho nhiều đối tượng khác nhau qua mạng. Việc mất mát, rò rỉ thông tin có thể ảnh hưởng nghiêm trọng đến tài nguyên thông tin, tài chính, danh tiếng của tổ chức, cá nhân. Vì vậy nhu cầu bảo vệ thông tin được đặt lên hàng đầu trong việc bảo mật và an toàn mạng**.**

2.1 Sự cần thiết của an toàn thông tin

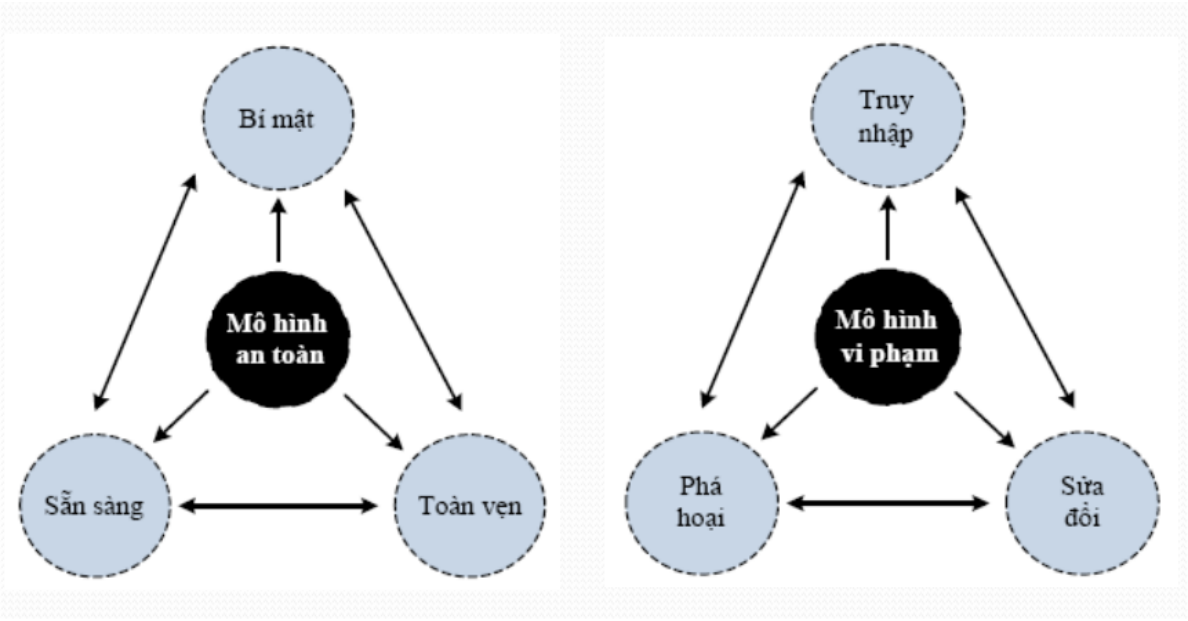
Hệ thống thông tin là thành phần thiết yếu trong mọi cơ quan, tổ chức và đem lại khả năng xử lý thông tin, là tài sản quan trọng nhưng hệ thống thông tin cũng chứa rất nhiều điểm yếu và rủi do. Do máy tính được phát triển với tốc độ rất nhanh để đáp ứng nhiều yêu cầu của người dùng, các phiên bản được phát hành liên tục với các tính năng mới được thêm vào ngày càng nhiều, điều này làm cho các phần mềm không được kiểm tra kỹ trước khi phát hành và bên trong chúng chứa rất nhiều lỗ hổng có thể dễ dàng bị lợi dụng. Thêm vào đó là việc phát triển của hệ thống mạng, cũng như sự phân tán của hệ thống thông tin, làm cho người dùng truy cập thông tin dễ dàng hơn và tin tặc cũng có nhiều mục tiêu tấn công dễ dàng hơn.

2.2.Mục đích của an toàn thông tin

Các hệ thống máy tính lưu giữ rất nhiều thông tin và tài nguyên cần được bảo vệ. Trong một tổ chức, những thông tin và tài nguyên này có thể là dữ liệu kế toán, thông tin nguồn nhân lực, thông tin quản lý, bán hàng, nghiên cứu, sáng chế, phân phối, thông tin về tổ chức và thông tin về các hệ thống nghiên cứu. Các tấn công vào hệ thống có thể xuất phát từ những đối thủ của tổ chức hoặc cá nhân do đó, các phương pháp để bảo đảm an toàn cho những thông tin này có thể rất phức tạp và nhạy cảm. Các cuộc tấn công có thể xuất phát từ nhiều nguồn khác nhau, cả từ bên trong và bên ngoài tổ chức. Hậu quả mà những tấn công thành công để lại sẽ rất nghiêm trọng.

Bảo đảm tính riêng tư: Các hệ thống máy tính lưu giữ rất nhiều thông tin cá nhân cần được giữ bí mật. Những thông tin này bao gồm: Số thẻ bảo hiểm xã hội, số thẻ ngân hàng, số thẻ tín dụng, thông tin về gia đình,… Tính riêng tư là yêu cầu rất quan trọng mà các ngân hàng, các công ty tín dụng, các công ty đầu tư và các hãng khác cần phải đảm bảo để gửi đi các tài liệu thông tin chi tiết về

cách họ sử dụng và chia sẻ thông tin về khách hàng. Các nơi này có những quy định bắt buộc để bảo đảm những thông tin cá nhân được bí mật và bắt buộc phải thực hiện những quy định đó để bảo đảm tính riêng tư. Hậu quả nghiêm trọng sẽ xảy ra nếu một kẻ giả mạo truy nhập được những thông tin cá nhân.



Hình 1-1.Các mục đích của an toàn thông tin

2.3.Các nguy cơ mất an toàn thông tin

Nguy cơ mất an toàn thông tin về khía cạnh vật lý: là nguy cơ do mất điện, nhiệt độ, độ ẩm không đảm bảo, hỏa hoạn, thiên tai, thiết bị phần cứng bị hư hỏng, các phần tử phá hoại như nhân viên xấu bên trong và kẻ trộm bên ngoài

Nguy cơ bị mất, hỏng, sửa đổi nội dung thông tin: Người dùng có thể vô tình để lộ mật khẩu hoặc không thao tác đúng quy trình tạo cơ hội cho kẻ xấu lợi dụng để lấy cắp hoặc làm hỏng thông tin.

Nguy cơ bị tấn công bởi các phần mềm độc hại: Các phần mềm độc hại tấn công bằng nhiều phương pháp khác nhau để xâm nhập vào hệ thống với các mục đích khác nhau như: virus, sâu máy tính (Worm), phần mềm gián điệp (Spyware),...

Nguy cơ xâm nhập từ lỗ hổng bảo mật Lỗ hổng bảo mật thường là do lỗi lập trình, lỗi hoặc sự cố phần mềm, nằm trong một hoặc nhiều thành phần tạo nên hệ điều hành hoặc trong chương trình cài đặt trên máy tính

Nguy cơ mất an toàn thông tin do sử dụng e-mail: Tấn công có chủ đích bằng thư điện tử là tấn công bằng email giả mạo giống như email được gửi từ người quen, có thể gắn tập tin đính kèm nhằm làm cho thiết bị bị nhiễm virus.

2.4.Các giải pháp bảo vệ an toàn thông tin

Bảo vệ thông tin về mặt vật lý: Để bảo vệ an toàn thông tin của hệ thống cần có các thiết bị và biện pháp phòng chống các nguy cơ gây mất an toàn thông

tin về khía cạnh vật lý như: gắn thiết bị lưu điện, thường xuyên sao lưu dữ liệu. Sử dụng các chính sách vận hành hệ thống đúng quy trình, an toàn và bảo mật

Bảo vệ với nguy cơ mất thông tin: Cung cấp những hướng dẫn, những quy tắc, và những quy trình để thiết lập một môi trường thông tin an toàn.

Bảo vệ với nguy cơ bị tấn công bởi các phần mềm độc hại:

+ Cập nhập hệ điều hành của máy tính, phần mềm máy tính cũng phải được cập nhật với phiên bản mới nhất. Là phiên bản thường chứa bản sửa lỗi bảo mật hơn để ngăn chặn phần mềm độc hại tấn công.
+ Sử dụng phần mềm diệt virus
+ Sử dụng phương thức chứng thực tên truy cập và mật khẩu
+ Không mở bất kỳ tập tin đính kèm được gửi từ một địa chỉ e-mail mà không biết rõ hoặc không tin tưởng
+ Bảo vệ hệ thống bằng tường lửa (firewall)

Mã hóa thông tin

3. TÓM TẮT NỘI DUNG

- Khái niệm về an toàn thông tin, bảo mật thông tin
- Khái niệm về an ninh mạng máy tính
- Sự cần thiết của an toàn thông tin
- Nguy cơ mất an toàn thông tin
- Cách thức bảo mật an toàn thông tin

4. CÂU HỎI

Câu 1: Trình bày các khái niệm về an toàn thông tin và bảo mật thông tin.

Câu 2:Nêu vai trò của an toàn thông tin và bảo mật thông tin.

Câu 3:Nêu các ví dụ về bảo mật an toàn thông tin

Câu 4: Trình bày các dịch vụ an toàn mạng (confidentiality, authentication, integrity, nonrepudiation, access control, availability).

Câu 5: Nêu các yêu cầu cũng như mục tiêu của việc đảm bảo an toàn và bảo mật thông tin

BÀI 2: MÃ HÓA THÔNG TIN

Mã bài MĐ 26-02

Thời gian : 7 giờ

I. MỤC TIÊU: Sau khi học bài học này, sinh viên có khả năng

- Liệt kê và phân biệt được các kiểu mã hóa dữ liệu
- Áp dụng được việc mã hóa và giải mã với một số phương pháp cơ bản
- Trình bày về hạ tầng ứng dụng khóa công khai
- Thực hành cài đặt, cấu hình bộ lọc gói tin bảo mật dữ liệu
- Thực hiện các thao tác an toàn với máy tính

II. NỘI DUNG CHÍNH

1. Căn bản về mã hoá

Mục tiêu : Liệt kê và phân biệt được các kiểu mã hóa dữ liệu

1.1.Tại sao cần phải mã hoá

Thuật toán Cryptography đề cập tới nghành khoa học nghiên cứu về mã hoá và giải mã thông tin. Cụ thể hơn là nghiên cứu các cách thức chuyển đổi thông tin từ dạng rõ (clear text) sang dạng mờ (cipher text) và ngược lại. Đây là một phương pháp hỗ trợ rất tốt cho trong việc chống lại những truy cập bất hợp pháp tới dữ liệu được truyền đi trên mạng, áp dụng mã hoá sẽ khiến cho nội dung thông tin được truyền đi dưới dạng mờ và không thể đọc được đối với bất kỳ ai cố tình muốn lấy thông tin đó.

1.2.Nhu cầu sử dụng kỹ thuật mã hoá

Nhu cầu về sử dụng mã hoá xuất hiện khi các bên tham gia trao đổi thông tin muốn bảo vệ các tài liệu quan trọng hay gửi chúng đi một cách an toàn. Các tài liệu quan trọng có thể là: tài liệu quân sự, tài chính, kinh doanh hoặc đơn giản là một thông tin nào đó mang tính riêng tư.

1.3.Quá trình mã hoá

Mã hoá tức là nói đến việc che dấu thông tin bằng cách sử dụng thuật toán. Che dấu ở đây không phải là làm cho thông tin biến mất mà là cách thức chuyển từ dạng tỏ sang dạng mờ. Một thuật toán là một tập hợp của các câu lệnh mà theo đó chương trình sẽ biết phải làm thế nào để xáo trộn hay phục hồi lại dữ liệu. Chẳng hạn một thuật toán rất đơn giản mã hoá thông điệp cần gửi đi như sau:

Bước 1: Thay thế toàn bộ chữ cái “e” thành số “3”

Bước 2: Thay thế toàn bộ chữ cái “a” thành số “4”

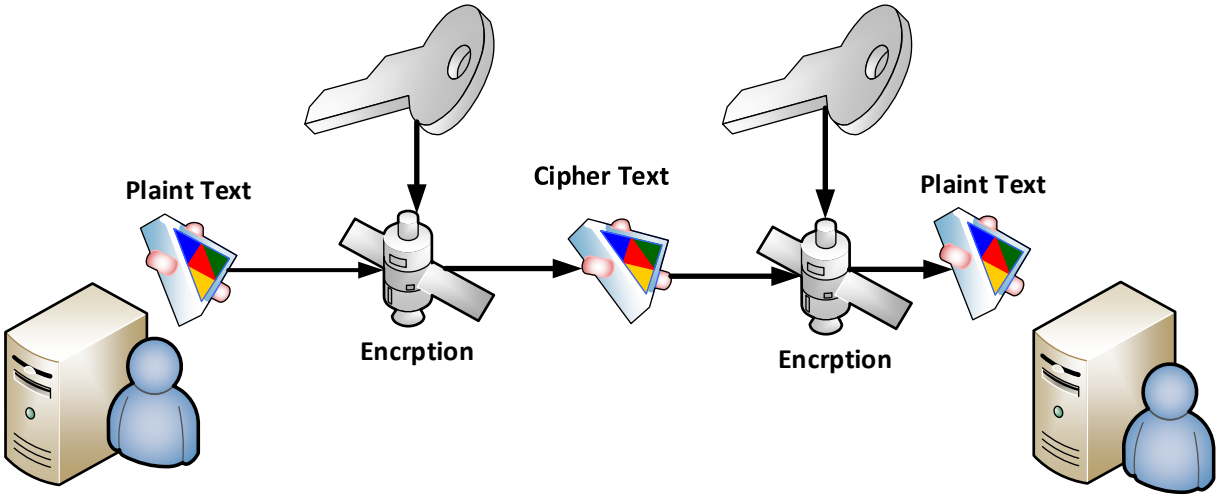
Bước 3: Đảo ngược thông điệp

Trên đây là một ví dụ rất đơn giản mô phỏng cách làm việc của một thuật toán mã hoá. Sau đây là các thuật ngữ cơ bản nhất giúp chúng ta nắm được các khái niệm:

+ Sender/Receiver: Người gửi/Người nhận dữ liệu
+ Plaintext (Cleartext): Thông tin trước khi được mã hoá. Đây là dữ liệu ban đầu ở dạng rõ
+ Ciphertext: Thông tin, dữ liệu đã được mã hoá ở dạng mờ
+ Key: Thành phần quan trọng trong việc mã hoá và giải mã
+ CryptoGraphic Algorithm: Là các thuật toán được sử dụng trong việc mã hoá hoặc giải mã thông tin
+ CryptoSystem: Hệ thống mã hoá bao gồm thuật toán mã hoá, khoá, Plaintext, Ciphertext
+ Kí hiệu chung: P là thông tin ban đầu, trước khi mã hoá. E() là thuật toán mã hoá. D() là thuật toán giải mã. C là thông tin mã hoá. K là khoá. Chúng ta biểu diễn quá trình mã hoá và giải mã như sau:

Quá trình mã hoá được mô tả bằng công thức: EK(P)=C

Quá trình giải mã được mô tả bằng công thức: DK(C)=P



Hình 2-1:Sơ đồ quá trình mã hóa và giải mã

Bên cạnh việc làm thế nào để che dấu nội dung thông tin thì mã hoá phải đảm bảo các mục tiêu sau:

a. **Confidentiality (Tính bí mật)**: Đảm bảo dữ liệu được truyền đi một cách an toàn và không thể bị lộ thông tin nếu như có ai đó cố tình muốn có được nội dung của dữ liệu gốc ban đầu. Chỉ những người được phép mới có khả năng đọc được nội dung thông tin ban đầu.

b. **Authentication (Tính xác thực):** Giúp cho người nhận dữ liệu xác định được chắc chắn dữ liệu mà họ nhận là dữ liệu gốc ban đầu. Kẻ giả mạo không thể có khả năng để giả dạng một người khác hay nói cách khác không thể mạo danh để gửi dữ liệu. Người nhận có khả năng kiểm tra nguồn gốc thông tin mà họ nhận được.

c. **Integrity (Tính toàn vẹn):** Giúp cho người nhận dữ liệu kiểm tra được rằng dữ liệu không bị thay đổi trong quá trình truyền đi. Kẻ giả mạo không thể có khả năng thay thế dữ liệu ban đầu băng dữ liệu giả mạo

d. **Non-repudation (Tính không thể chối bỏ)**: Người gửi hay người nhận không thể chối bỏ sau khi đã gửi hoặc nhận thông tin.

2. Độ an toàn của thuật toán

Mục tiêu : Áp dụng được việc mã hóa và giải mã với một số phương pháp cơ bản

Nguyên tắc đầu tiên trong mã hoá là "Thuật toán nào cũng có thể bị phá vỡ". Các thuật toán khác nhau cung cấp mức độ an toàn khác nhau, phụ thuộc vào độ phức tạp để phá vỡ chúng. Tại một thời điểm, độ an toàn của một thuật toán phụ thuộc:

+ Nếu chi phí hay phí tổn cần thiết để phá vỡ một thuật toán lớn hơn giá trị của thông tin đã mã hóa thuật toán thì thuật toán đó tạm thời được coi là an toàn.
+ Nếu thời gian cần thiết dùng để phá vỡ một thuật toán là quá lâu thì thuật toán đó tạm thời được coi là an toàn.
+ Nếu lượng dữ liệu cần thiết để phá vỡ một thuật toán quá lơn so với lượng dữ liệu đã được mã hoá thì thuật toán đó tạm thời được coi là an toàn

3. Phân loại các thuật toán mã hoá

Mục tiêu : Trình bày về hạ tầng ứng dụng khóa công khai

Có rất nhiều các thuật toán mã hoá khác nhau. Từ những thuật toán được công khai để mọi người cùng sử dụng và áp dụng như là một chuẩn chung cho việc mã hoá dữ liệu; đến những thuật toán mã hoá không được công bố. Có thể phân loại các thuật toán mã hoá như sau:

Phân loại theo các phương pháp:

+ Mã hoá cổ điển (Classical cryptography)
+ Mã hoá đối xứng (Symetric cryptography)
+ Mã hoá bất đối xứng(Asymetric cryptography)
+ Hàm băm (Hash function)
+ Phân loại theo số lượng khoá:
+ Mã hoá khoá bí mật (Private-key Cryptography)

+ Mã hoá khoá công khai (Public-key Cryptography)

3.1 Mã hoá cổ điển

Trong mã hoá cổ điển có 02 phương pháp nổi bật đó là:

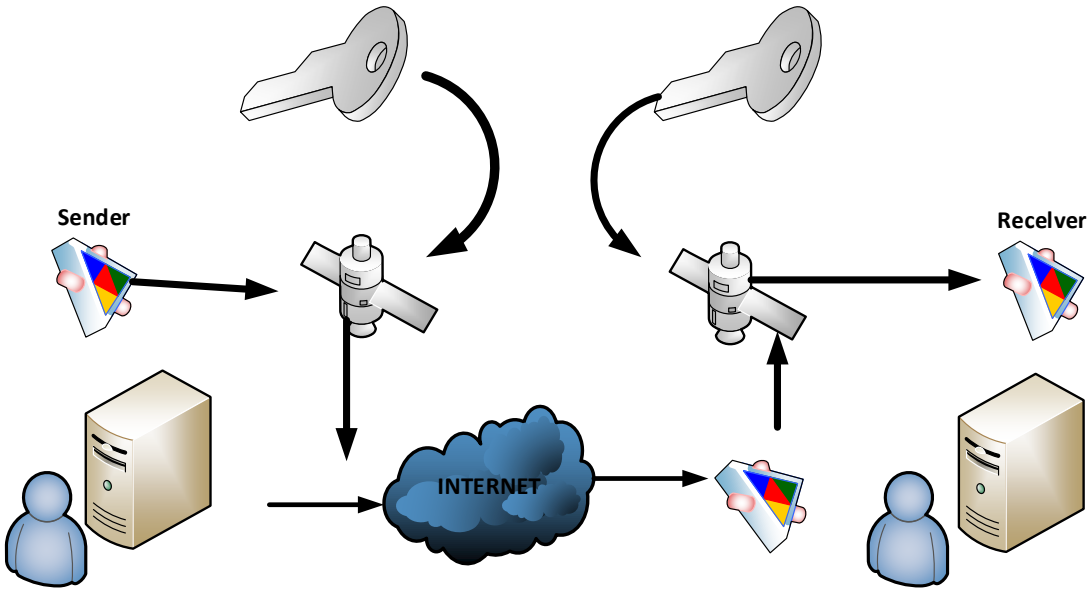
Mã hoá thay thế (Substitution Cipher):Là phương pháp mà từng kí tự (hay từng nhóm kí tự) trong bản rõ (Plaintext) được thay thế bằng một kí tự (hay một nhóm kí tự) khác để tạo ra bản mờ (Ciphertext). Bên nhận chỉ cần đảo ngược trình tự thay thế trên Ciphertext để có được Plaintext ban đầu.

Mã hoá hoán vị (Transposition Cipher):Bên cạnh phương pháp mã hoá thay thế thì trong mã hoá cổ điển có một phương pháp khác nữa cũng nổi tiếng không kém, đó chính là mã hoá hoán vị. Nếu như trong phương pháp mã hoá thay thế, các kí tự trong Plaintext được thay thế hoàn toàn bằng các kí tự trong Ciphertext, thì trong phương pháp mã hoá hoán vị, các kí tự trong Plaintext vẫn được giữ nguyên, chúng chỉ được sắp xếp lại vị trí để tạo ra Ciphertext. Tức là các kí tự trong Plaintext hoàn toàn không bị thay đổi bằng kí tự khác.

3.2 Mã hoá đối xứng

Mã hoá đối xứng còn có một số tên gọi khác như Secret Key Cryptography (hay Private Key Cryptography), sử dụng cùng một khoá cho cả hai quá trình mã hoá và giải mã.

Quá trình thực hiện như sau:



Hình 2-2:sơ đồ mã hóa đối xứng một khóa

Hình vẽ trên chính là quá trình tiến hành trao đổi thông tin giữa bên gửi và bên nhận thông qua việc sử dụng phương pháp mã hoá đối xứng. Trong quá trình này, thì thành phần quan trọng nhất cần phải được giữ bí mật chính là khoá. Việc trao đổi, thoả thuận về thuật toán được sử dụng trong việc mã hoá có

thể tiến hành một cách công khai, nhưng bước thoả thuận về khoá trong việc mã hoá và giải mã phải tiến hành bí mật.

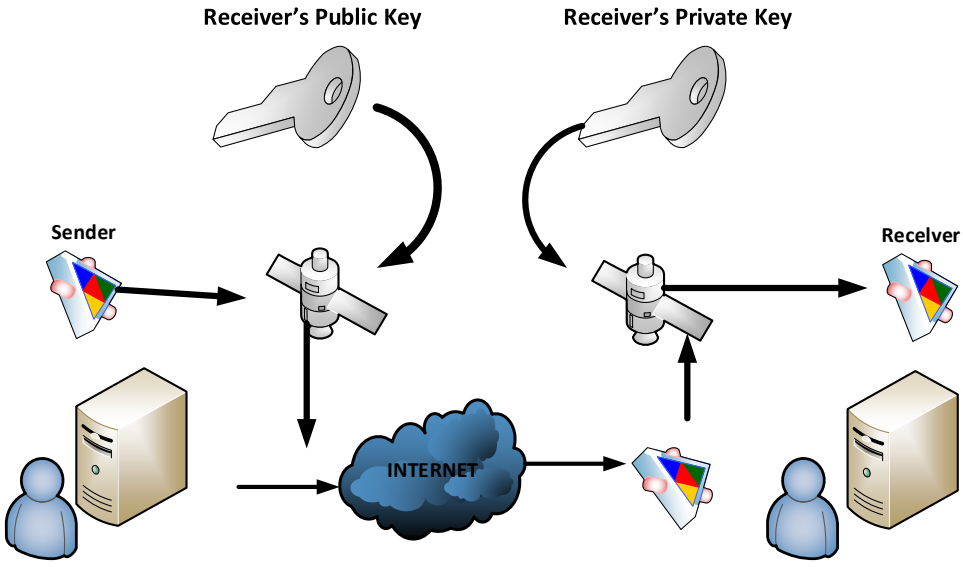
Mã hoá đối xứng có thể được phân thành 02 loại:

Loại thứ nhất tác động trên bản rõ theo từng nhóm bits. Từng nhóm bits này được gọi với một cái tên khác là khối (Block) và thuật toán được áp dụng gọi là Block Cipher. Theo đó, từng khối dữ liệu trong văn bản ban đầu được thay thế bằng một khối dữ liệu khác có cùng độ dài. Đối với các thuật toán ngày nay thì kích thước chung của một Block là 64 bits.

Loại thứ hai tác động lên bản rõ theo từng bit một. Các thuật toán áp dụng được gọi là Stream Cipher. Theo đó, dữ liệu của văn bản được mã hoá từng bit một. Các thuật toán mã hoá dòng này có tốc độ nhanh hơn các thuật toán mã hoá khối và nó thường được áp dụng khi lượng dữ liệu cần mã hoá chưa biết trước.Một số thuật toán nổi tiếng trong mã hoá đối xứng là: DES, Triple DES(3DES), RC4, AES…

3.3 Mã hoá bất đối xứng

Hay còn được gọi với một cái tên khác là mã hoá khoá công khai (Public Key Cryptography), nó được thiết kế sao cho khoá sử dụng trong quá trình mã hoá khác biệt với khoá được sử dụng trong quá trình giải mã. Hơn thế nữa, khoá sử dụng trong quá trình giải mã không thể được tính toán hay luận ra được từ khoá được dùng để mã hoá và ngược lại, tức là hai khoá này có quan hệ với nhau về mặt toán học nhưng không thể suy diễn được ra nhau. Thuật toán này được gọi là mã hoá công khai vì khoá dùng cho việc mã hoá được công khai cho tất cả mọi người. Một người bất kỳ có thể dùng khoá này để mã hoá dữ liệu nhưng chỉ duy nhất người mà có khoá giải mã tương ứng mới có thể đọc được dữ liệu mà thôi. Do đó trong thuật toán này có 2 loại khoá: Khoá để mã hoá được gọi là Public Key, khoá để giải mã được gọi là Private Key.



Hình 2-3:sơ đồ mã đối xứng 2 khóa

Mã hoá khoá công khai ra đời để giải quyết vấn đề về quản lý và phân phối khoá của các phương pháp mã hoá đối xứng. Hình minh hoạ ở trên cho chúng ta thấy được quá trình truyền tin an toàn dựa vào hệ thống mã hoá khoá công khai. Quá trình truyền và sử dụng mã hoá khoá công khai được thực hiện như sau:

Bên gửi yêu cầu cung cấp hoặc tự tìm khoá công khai của bên nhận trên một server chịu trách nhiệm quản lý khoá.

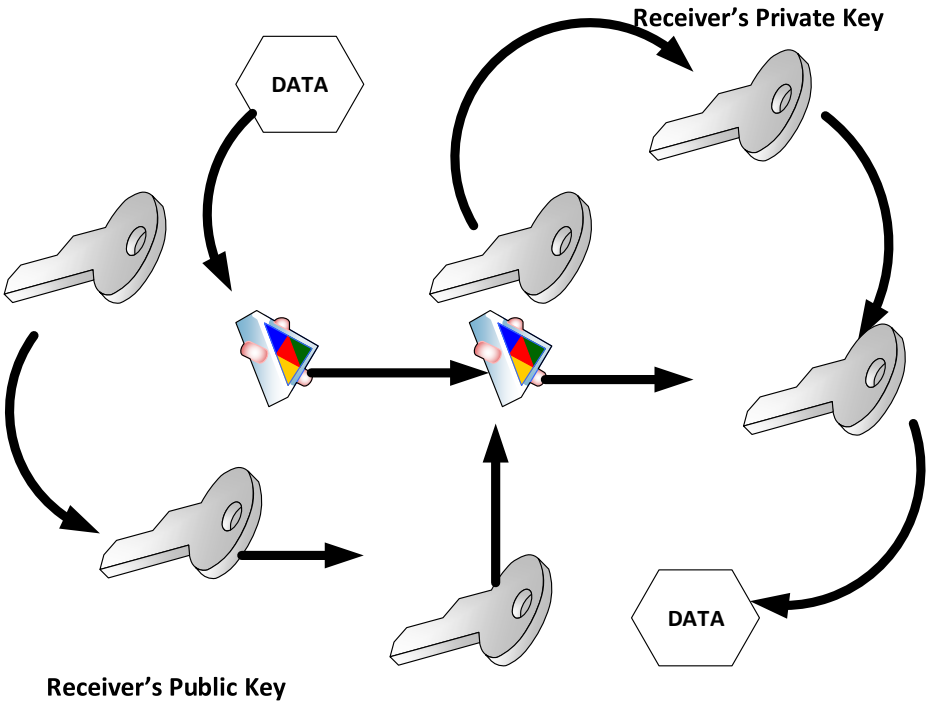
Sau đó hai bên thống nhất thuật toán dùng để mã hoá dữ liệu, bên gửi sử dụng khoá công khai của bên nhận cùng với thuật toán đã thống nhất để mã hoá thông tin được gửi đi.

Khi nhận được thông tin đã mã hoá, bên nhận sử dụng khoá bí mật của mình để giải mã và lấy ra thông tin ban đầu.

3.4 Hệ thống mã hoá khoá lai (Hybrid Cryptosystems)

Trên thực tế hệ thống mã hoá khoá công khai chưa thể thay thế hệ thống mã hoá khoá bí mật được, nó ít được sử dụng để mã hoá dữ liệu mà thường dùng để mã hoá khoá. Hệ thống mã hoá khoá lai ra đời là sự kết hợp giữa tốc độ và tính an toàn của hai hệ thống mã hoá ở trên. Dưới đây là mô hình của hệ thống mã hoá lai:

Nhìn vào mô hình chúng ta có thể hình dung được hoạt động của hệ thống mã hoá này như sau



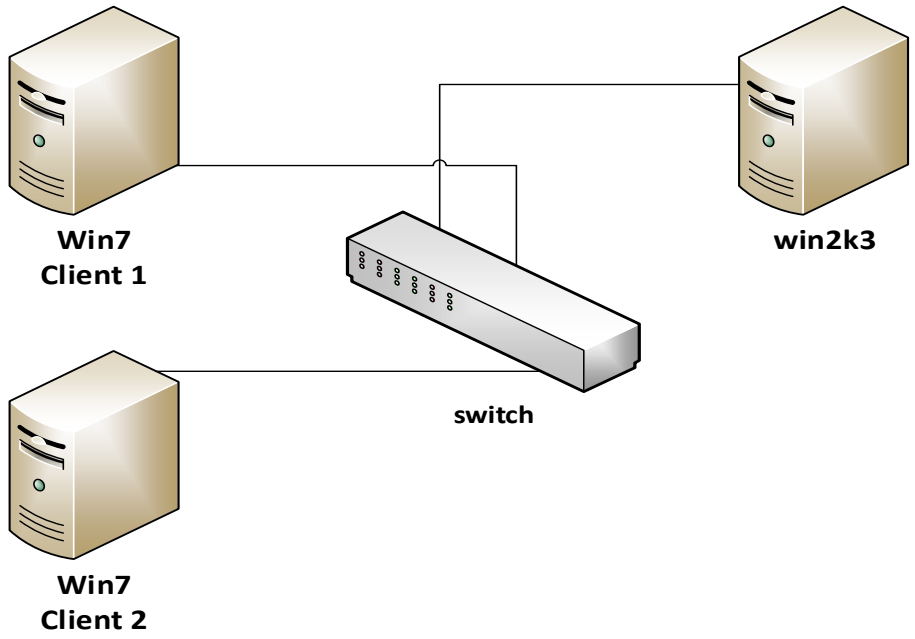
Hình 2-4:sơ đồ mã hóa lai

+ Bên gửi tạo ra một khoá bí mật dùng để mã hoá dữ liệu. Khoá này còn được gọi là Session Key.
+ Sau đó, Session Key này lại được mã hoá bằng khoá công khai của bên nhận dữ liệu.
+ Tiếp theo dữ liệu mã hoá cùng với Session Key đã mã hoá được gửi đi tới bên nhận.
+ Lúc này bên nhận dùng khoá riêng để giải mã Session Key và có được Session Key ban đầu.
+ Dùng Session Key sau khi giải mã để giải mã dữ liệu.

Như vậy, hệ thống mã hoá khoá lai đã tận dụng tốt được các điểm mạnh của hai hệ thống mã hoá ở trên đó là: tốc độ và tính an toàn. Điều này sẽ làm hạn chế bớt khả năng giải mã của tin tặc.

4. Bài tập thực hành

Bài tập 1: Cho mô hình mạng như sau**:**



Yêu cầu:Mã hóa thư mục dùng chung với gói lọc IPSec

Chuẩn bị

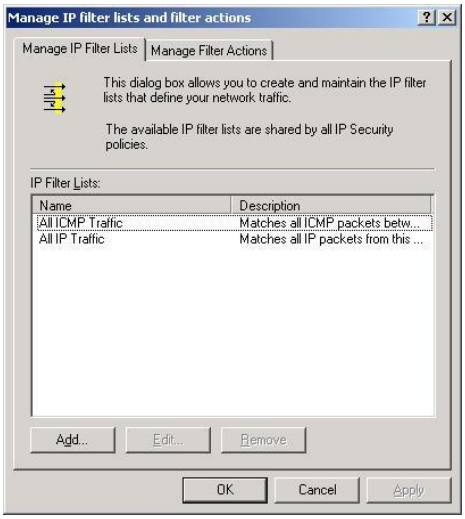
- 1 máy PC cài đặt win2k3 và nâng lên DC
- 2 máy PC cài đặt win7
- 1 switch
- 3 sợi cáp mạng bấm thẳng

Thực hiện

Các bước cài đặt

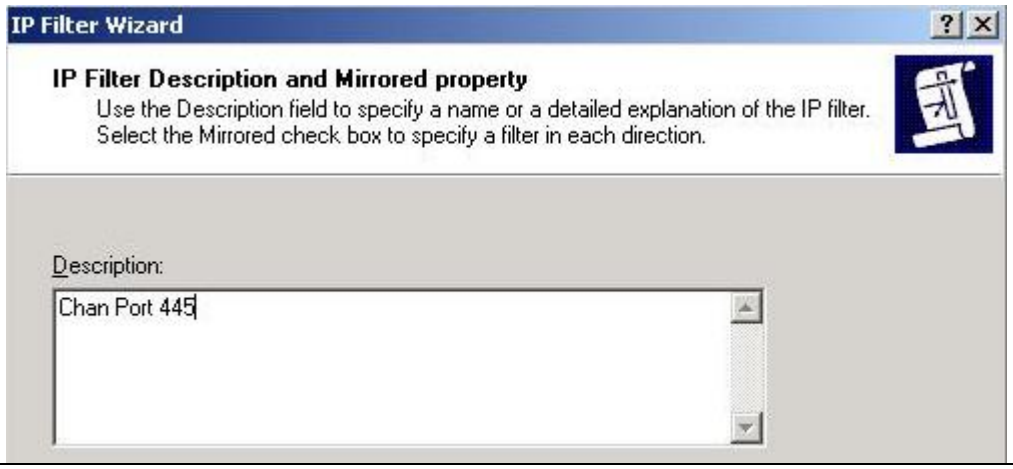
1.Xây dựng bộ lọc

Bước 1: Domain Security Policy →Right-Click vào IP Security Policy On Active Directory → Manage IP Filter Lists and Filter Actions…→OK

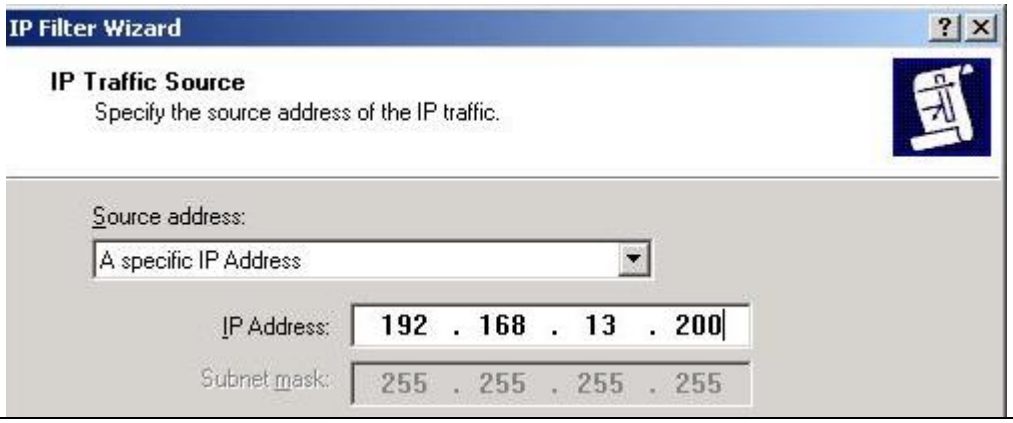

Manage IP filter lists and filter actions
Manage IP Filter Lists
Manage Filter Actions
This dialog box allows you to create and maintain the IP filter lists that define your network traffic.
The available IP filter lists are shared by all IP Security policies.
IP Filter Lists:
Name
Description
All ICMP Traffic
Matches all ICMP packets betw...
All IP Traffic
Matches all IP packets from this ...
Add...
Edit...
Remove
OK
Cancel
Apply

Kế tiếp →Add

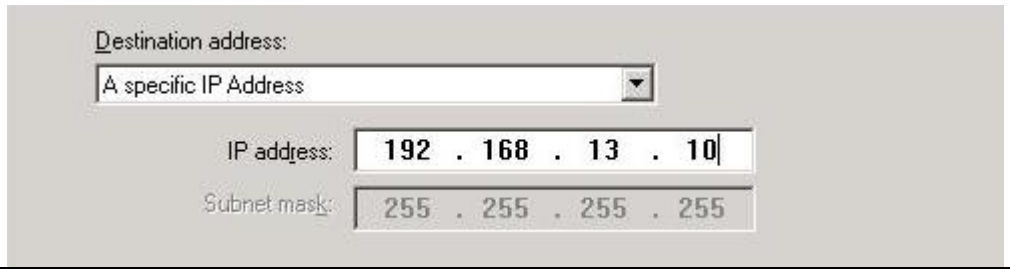
Bước 2: Đặt tên bộ lọc IP vào mục Name → Click Add để tạo IP Filter→Next


IP Filter Wizard
IP Filter Description and Mirrored property
Use the Description field to specify a name or a detailed explanation of the IP filter.
Select the Mirrored check box to specify a filter in each direction.
Description:
Chan Port 445

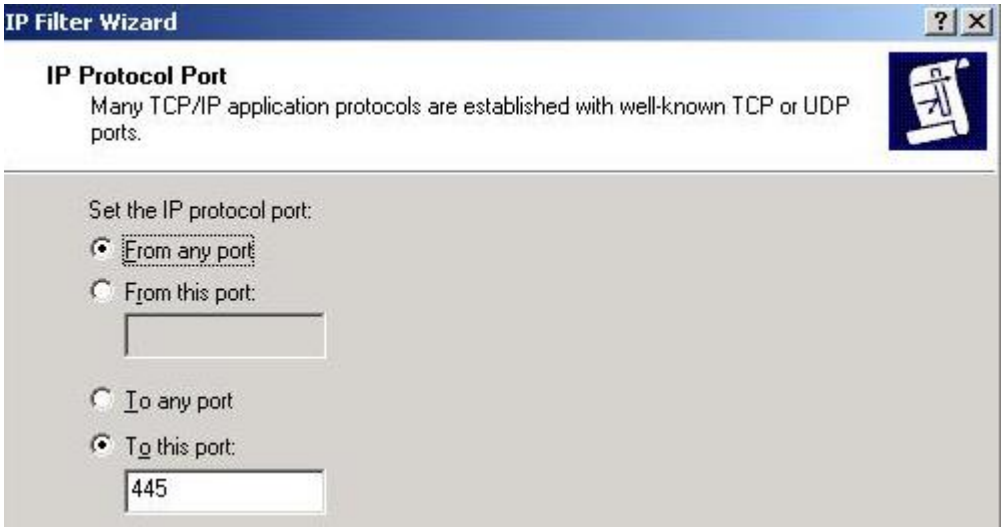
Bước 3: Thẻ Source Address→A Specific IP Address→Thẻ IP Address→ Nhập địa chỉ IP của máy muốn chặn truy cập→ Next


IP Filter Wizard
IP Traffic Source
Specify the source address of the IP traffic.
Source address:
A specific IP Address
IP Address:
192 . 168 . 13 . 200
Subnet mask:
255 . 255 . 255 . 255

Bước 4: Thẻ Source Address: chọn A Specific IP Address→thẻ IP Address→nhập địa chỉ IP của máy được truy cập đến→Next

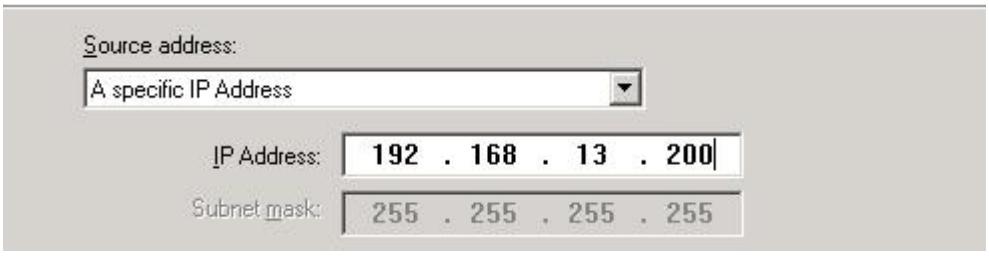


Bước 5: Thẻ Select A Protocol Type: →TCP → Next


IP Filter Wizard
IP Protocol Port
Many TCP/IP application protocols are established with well-known TCP or UDP ports.
Set the IP protocol port:
From any port
From this port:
To any port
To this port:
445

Kế tiếp → Thẻ To This Port: gõ vào 445 → Next→ Finish

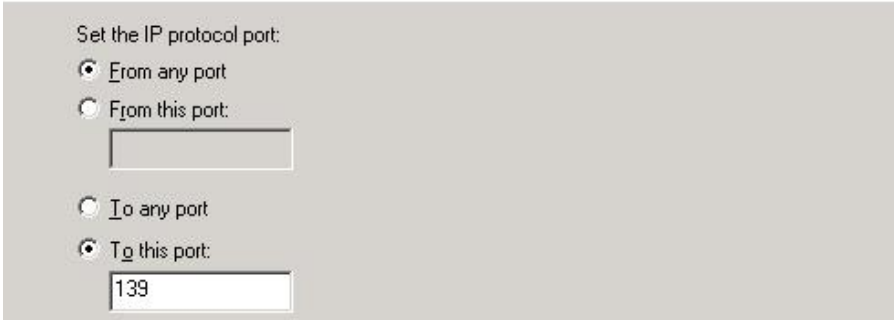
Bước 6: tạo thêm IP Filter → Add →Next →Next



Kế tiếp→ IP của máy muốn chặn truy cập →Next

Làm tương tự cho máy truy cập đến

Bước 7: Thẻ To This Port: gõ vào 139 → Next → Finish → OK

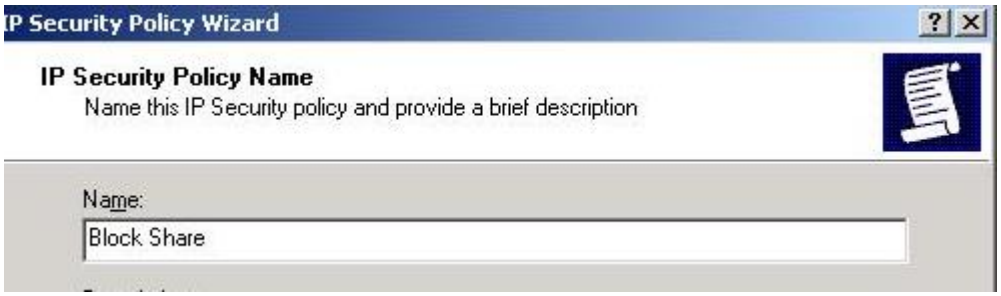


Kế tiếp → Tab Manager Filter Actions → Add → Next→ Gõ tên hành động vào mục Name → Next

Bước 8: Chọn Block → Next → Finish → Apply → OK.Hoàn thành việc xây dựng bộ lọc

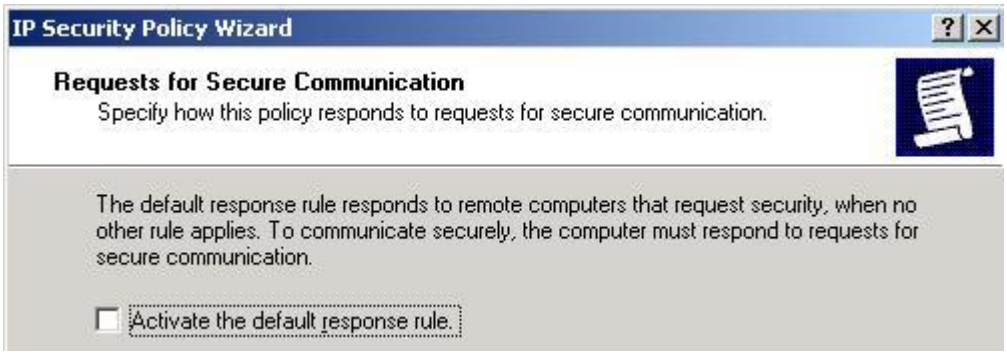
2.Thực thi bộ lọc

Bước 1: Domain Security Policy →Right-Click vào IP Security Policy On Active Directory → Create IP Security Policy **…**→Next


IP Security Policy Wizard
IP Security Policy Name
Name this IP Security policy and provide a brief description
Name:
Block Share

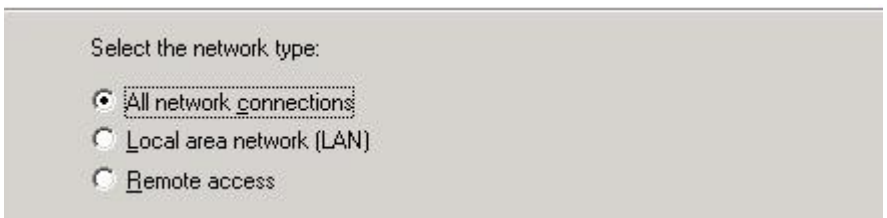
Kế tiếp→ Đặt tên cho IP Security → Next

Bước 2: Bỏ dấu check mục Activate the default response rule → Next → Finish

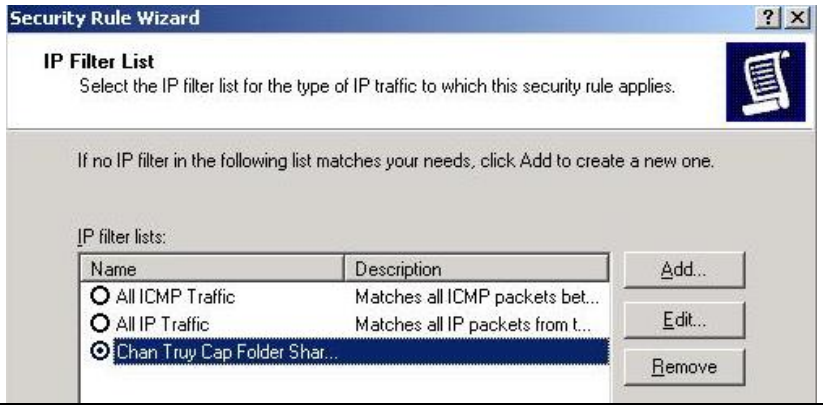

IP Security Policy Wizard
Requests for Secure Communication
Specify how this policy responds to requests for secure communication.
The default response rule responds to remote computers that request security, when no other rule applies. To communicate securely, the computer must respond to requests for secure communication.
Activate the default response rule.

Kế tiếp→Add→Next→Next

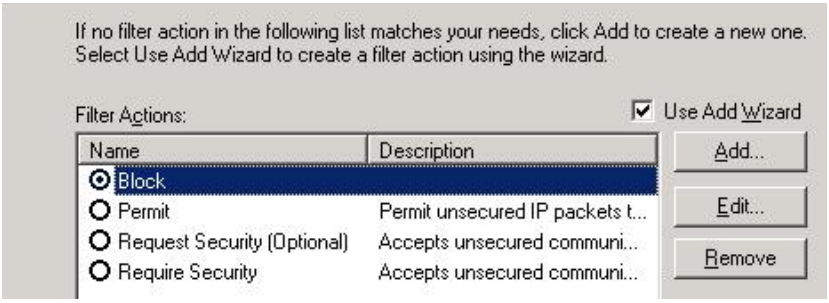
Bước 3: Chọn All Network Connections → Next



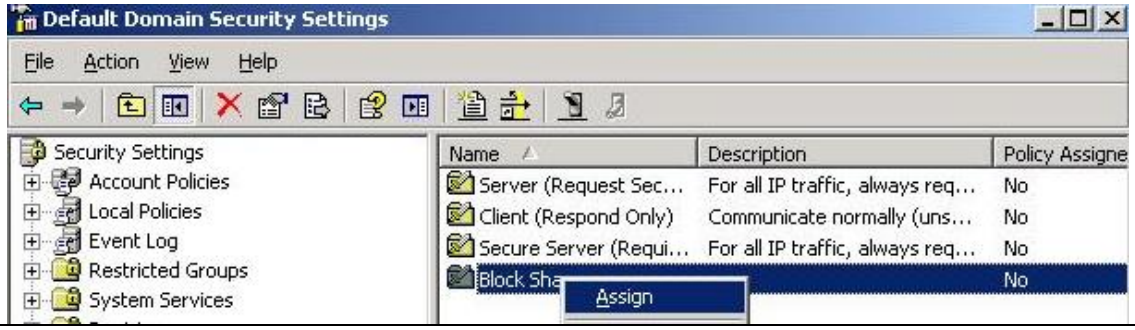
Bước 4: Chọn vào IP Filter muốn áp dụng → Next


Security Rule Wizard
IP Filter List
Select the IP filter list for the type of IP traffic to which this security rule applies.
If no IP filter in the following list matches your needs, click Add to create a new one.
IP filter lists:
Name
Description
All ICMP Traffic
Matches all ICMP packets bet...
All IP Traffic
Matches all IP packets from t...
Chan Truy Cap Folder Shar...
Add...
Edit...
Remove

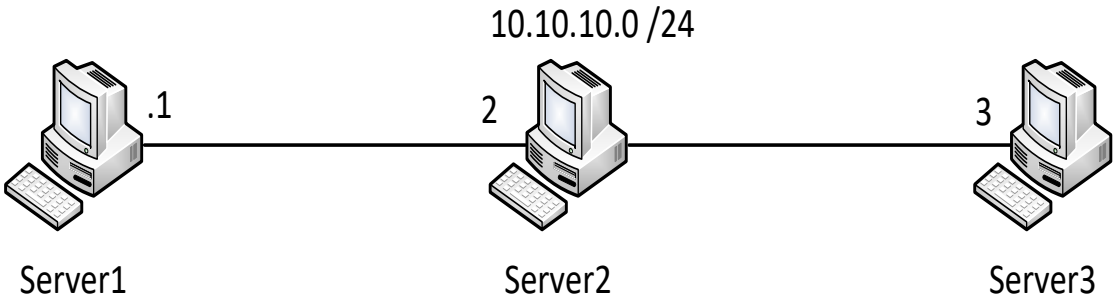
Bước 5: Chọn Filter Action muốn áp dụng → Next → Finish → OK



Bước 6: Right-Click vào IP Filter vừa tạo chọn Assign→Vào Run → gpupdate /force



Bài tập2 : cho mô hình mạng như sau:



Yêu cầu: Cài đặt, cấu hình bảo mật IP

Chuẩn bị:

- 3 máy PC cài đặt win2k3

- 2 sợi cáp bấm chéo

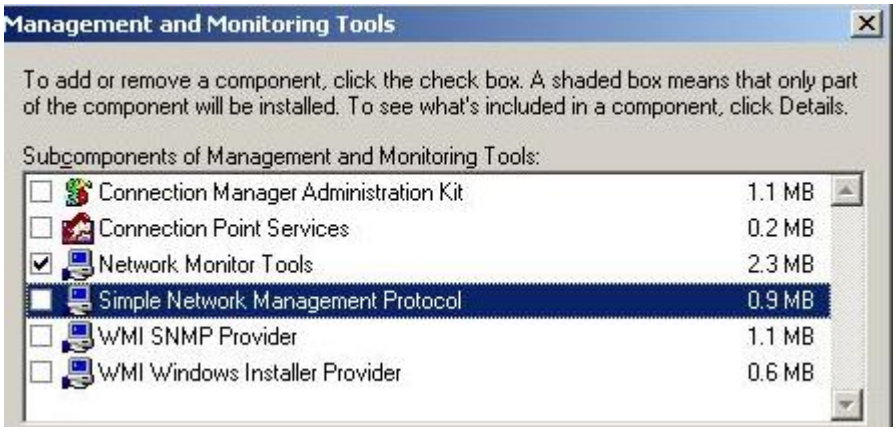
Thực hiện

Các bước cài đặt

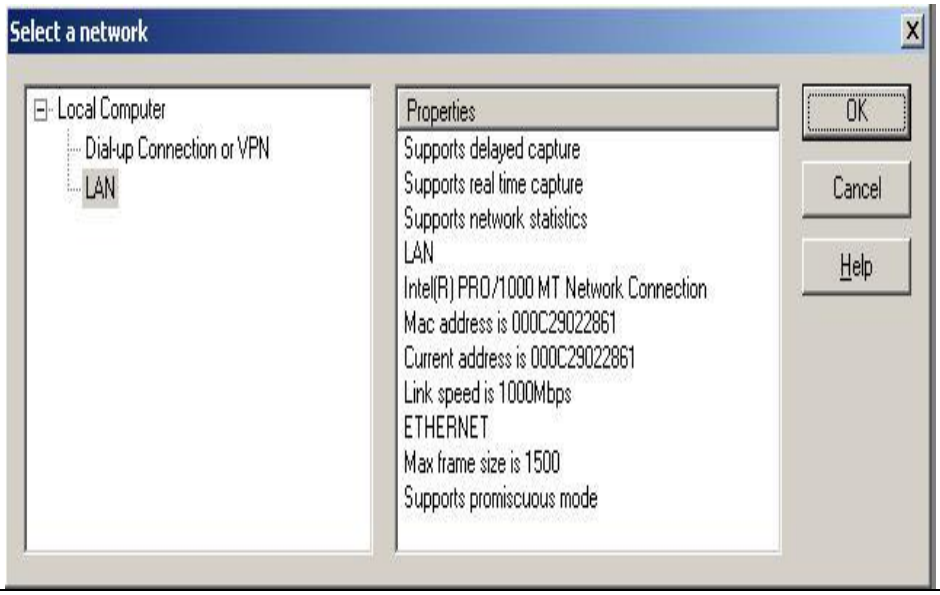
Bước 1: Control Panel → Add/Remove Program → Add/remove Windows Component → Management and Monitoring Tools → Details…→Next

Windows Components Wizard
Windows Components
You can add or remove components of Windows.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Management and Monitoring Tools 6.3 MB

Bước 2: Check vào Network Monitor Tools → OK → Next


Management and Monitoring Tools
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Management and Monitoring Tools:
Connection Manager Administration Kit 1.1 MB
Connection Point Services 0.2 MB
Network Monitor Tools 2.3 MB
Simple Network Management Protocol 0.9 MB
WMI SNMP Provider 1.1 MB
WMI Windows Installer Provider 0.6 MB

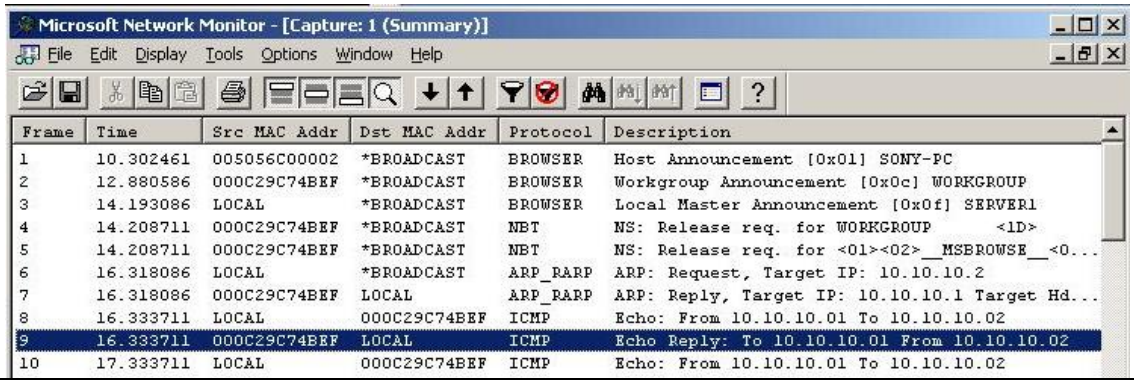
Bước 3: Network Monitor → OK→ Card Lan → OK



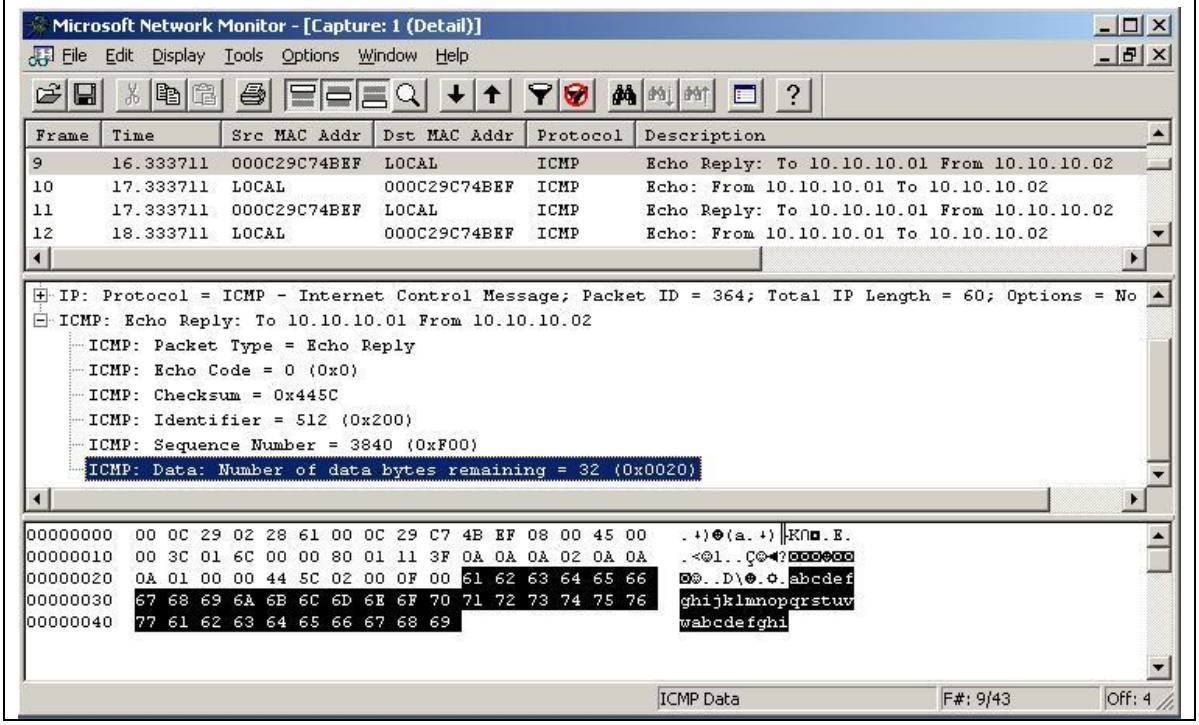
Bước 4: Microsoft network Monitor → Capture → Start để nguyên màn hình cả hai máy Server1 và Server2 ping địa chỉ với nhau

Bước 5: Trên Server1 →Capture → Stop and View

Bước 6: Click chọn dòng có Protocol là ICMP


Microsoft Network Monitor - [Capture: 1 (Summary)]
File Edit Display Tools Options Window Help
Frame Time Src MAC Addr Dst MAC Addr Protocol Description
1 10.302461 005056C00002 *BROADCAST BROWSER Host Announcement [0x01] SONY-PC
2 12.880586 000C29C74BEF *BROADCAST BROWSER Workgroup Announcement [0x0c] WORKGROUP
3 14.193086 LOCAL *BROADCAST BROWSER Local Master Announcement [0x0f] SERVER1
4 14.208711 000C29C74BEF *BROADCAST NBT NS: Release req. for WORKGROUP <1D>
5 14.208711 000C29C74BEF *BROADCAST NBT NS: Release req. for <01><02>__MSBROWSE__<0...
6 16.318086 LOCAL *BROADCAST ARP_RARP ARP: Request, Target IP: 10.10.10.2
7 16.318086 000C29C74BEF LOCAL ARP_RARP ARP: Reply, Target IP: 10.10.10.1 Target Hd...
8 16.333711 LOCAL 000C29C74BEF ICMP Echo: From 10.10.10.01 To 10.10.10.02
9 16.333711 000C29C74BEF LOCAL ICMP Echo Reply: To 10.10.10.01 From 10.10.10.02
10 17.333711 LOCAL 000C29C74BEF ICMP Echo: From 10.10.10.01 To 10.10.10.02

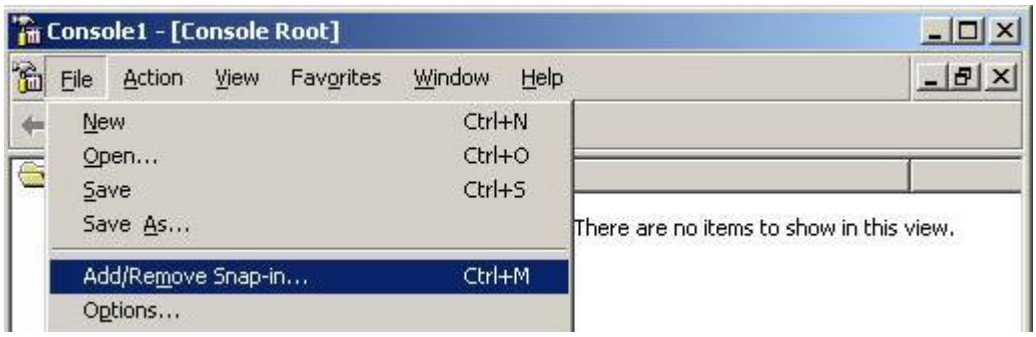
Bước 7: Click dấu "+" ICMP: Echo Reply → dòng ICMP: Data number of data bytes ramaining = 32


Microsoft Network Monitor - [Capture: 1 (Detail)]
File Edit Display Tools Options Window Help
Frame Time Src MAC Addr Dst MAC Addr Protocol Description
9 16.333711 000C29C74BEF LOCAL ICMP Echo Reply: To 10.10.10.01 From 10.10.10.02
10 17.333711 LOCAL 000C29C74BEF ICMP Echo: From 10.10.10.01 To 10.10.10.02
11 17.333711 000C29C74BEF LOCAL ICMP Echo Reply: To 10.10.10.01 From 10.10.10.02
12 18.333711 LOCAL 000C29C74BEF ICMP Echo: From 10.10.10.01 To 10.10.10.02
IP: Protocol = ICMP - Internet Control Message; Packet ID = 364; Total IP Length = 60; Options = No
ICMP: Echo Reply: To 10.10.10.01 From 10.10.10.02
ICMP: Packet Type = Echo Reply
ICMP: Echo Code = 0 (0x0)
ICMP: Checksum = 0x445C
ICMP: Identifier = 512 (0x200)
ICMP: Sequence Number = 3840 (0xF00)
ICMP: Data: Number of data bytes remaining = 32 (0x0020)
00000000 00 0C 29 02 28 61 00 0C 29 C7 4B EF 08 00 45 00
00000010 00 3C 01 6C 00 00 80 01 11 3F 0A 0A 0A 02 0A 0A
00000020 0A 01 00 00 44 5C 02 00 0F 00 61 62 63 64 65 66
00000030 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76
00000040 77 61 62 63 64 65 66 67 68 69
abcdef
ghijklmnopqrstuv
wabcdefghi
ICMP Data
F#: 9/43
Off: 4

Cấu hình

Bước 1: Thực hiện Trên Server1: (server2 làm tương tự)

Vào Start → Run → Gõ MMC →Console1 → chọn File → Add/Remove Snap-in…



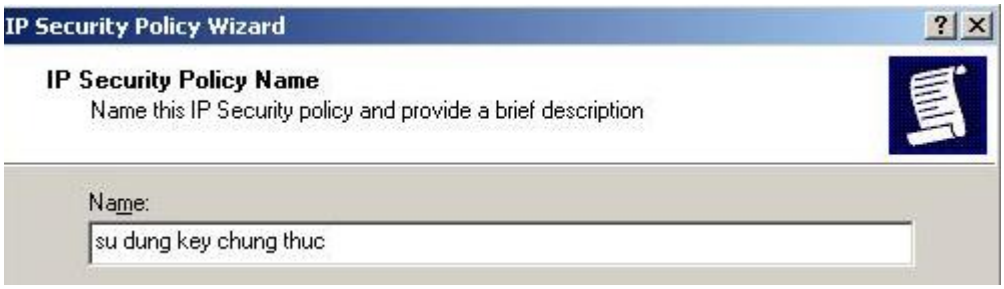
Add/Remove Snap-in → Add→ Chọn dòng IP Security Policy Management → Add → Close

Bước 2: Trong cửa sổ Select Computer or Domain → Local computer → Finish

Select Computer or Domain
Select which computer or domain this snap-in will manage
When this console is saved the location will also be saved
Local computer
The computer this console is running on

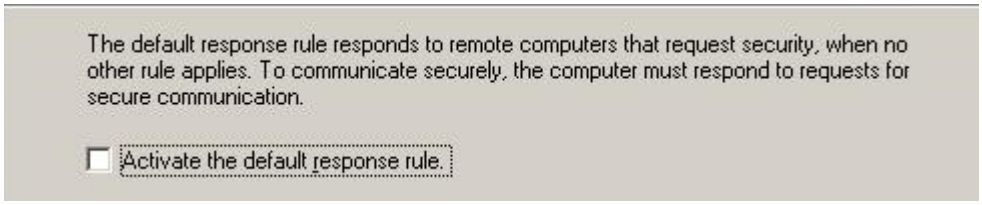
Tại hộp thoại Console1 → click phải chuột trên IP Security Policies on Local computer → Create IP Security Policy

Bước 3: Hộp thoại Welcome to the IP Security Policy Wizard → Next


IP Security Policy Wizard
IP Security Policy Name
Name this IP Security policy and provide a brief description
Name:
su dung key chung thuc

Kế tiếp→ IP Security Policy Name: gõ " su dung key chung thuc" → Next

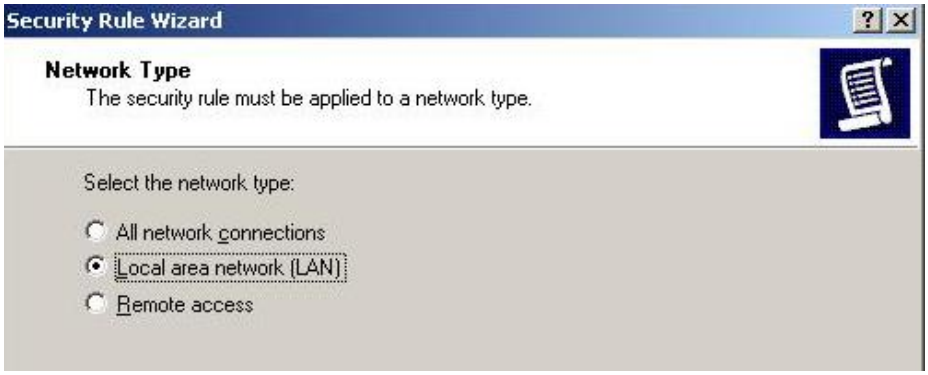
Bước 4: Bỏ check Activate the default response rule → Next→Next


The default response rule responds to remote computers that request security, when no other rule applies. To communicate securely, the computer must respond to requests for secure communication.
Activate the default response rule.

Hộp thoại Security rules … → Add→OK→Next→ this rule does not specify

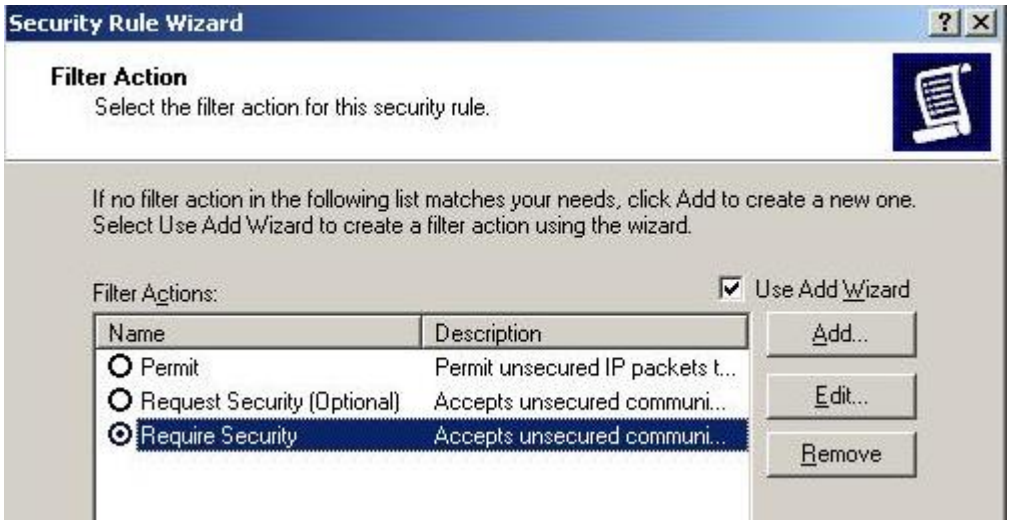
a tunnel → Next

Bước 5: Hộp thoại Netwok Type → Local area network (Lan) → Next


Security Rule Wizard
Network Type
The security rule must be applied to a network type.
Select the network type:
All network connections
Local area network (LAN)
Remote access

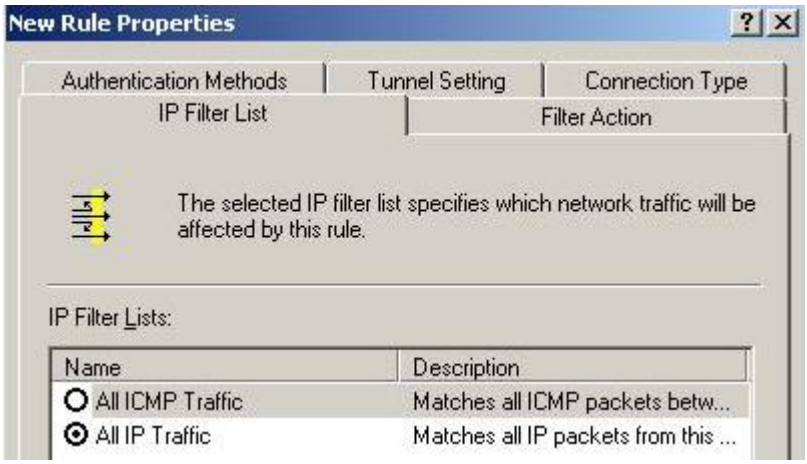
Kế tiếp→→ All IP Trafic → Next

Bước 6: Hộp thoại Filter Action → Require Security → Next→Next



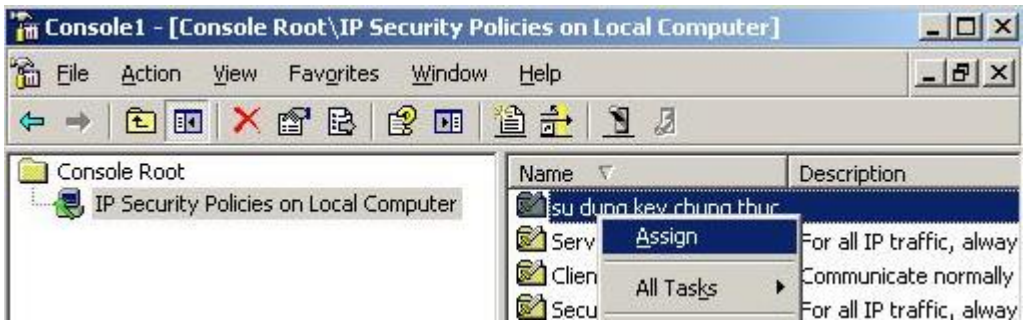
Hộp thoại Authentication Mothod → Use this string to .. →123+abc → Next

Bước 7: hộp thoại the seclect IP Filter … → chọn All IP Trafic →OK



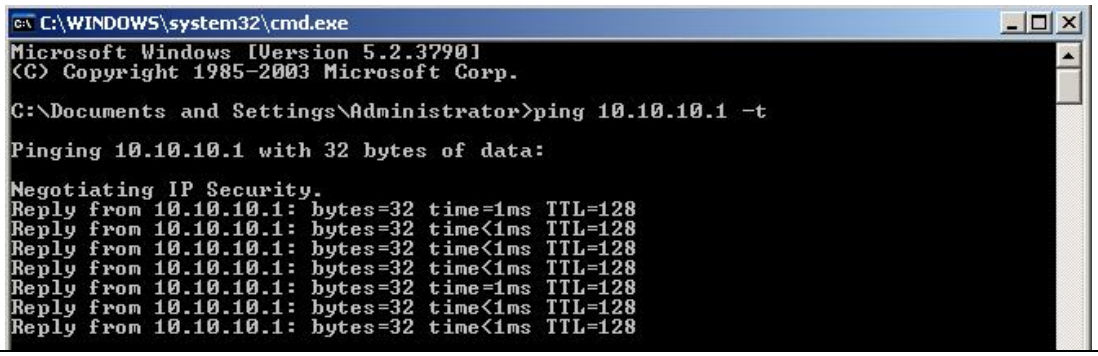
Hộp thoại Security rules for … → check vào All IP Trafic → OK

Bước 8: Click phải chuột trên " su dung key chung thuc" chọn Assign →gpupdate /force



Service → click phải chuột trên IPSEC Service → Restart

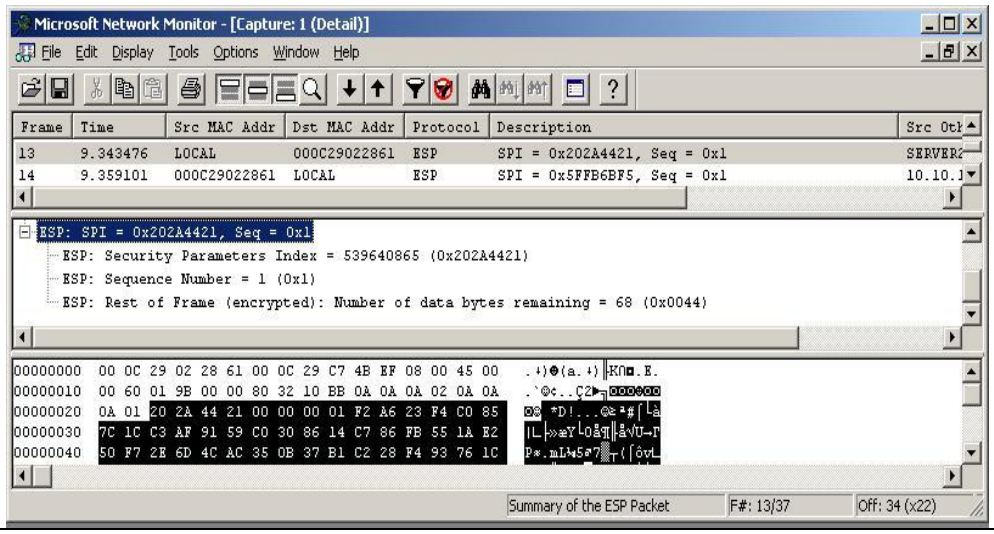
Bước 9: Thực hiện Trên Server2→ Network Monitor → Capture → Start→Ping địa chỉ IP của Server1 với tham số -t


C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
C:\Documents and Settings\Administrator>ping 10.10.10.1 -t
Pinging 10.10.10.1 with 32 bytes of data:
Negotiating IP Security.
Reply from 10.10.10.1: bytes=32 time=1ms TTL=128
Reply from 10.10.10.1: bytes=32 time<1ms TTL=128
Reply from 10.10.10.1: bytes=32 time<1ms TTL=128
Reply from 10.10.10.1: bytes=32 time<1ms TTL=128
Reply from 10.10.10.1: bytes=32 time=1ms TTL=128
Reply from 10.10.10.1: bytes=32 time<1ms TTL=128
Reply from 10.10.10.1: bytes=32 time<1ms TTL=128

Bước 10: màn hình Network Monitor của server2 → Capture → Stop and View → →Protocol là ESP

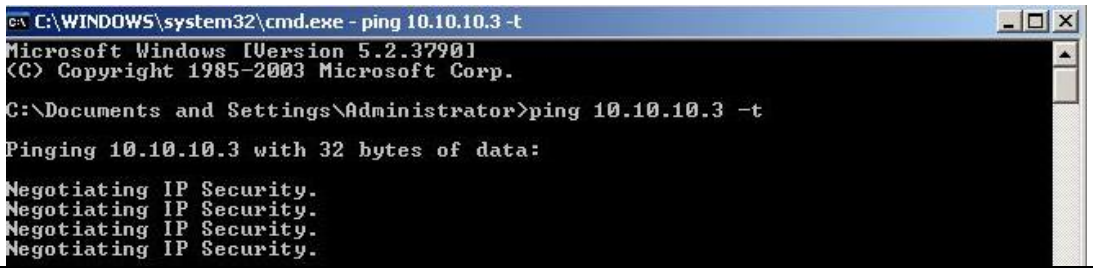
Microsoft Network Monitor - [Capture: 1 (Summary)]
File Edit Display Tools Options Window Help
Frame Time Src MAC Addr Dst MAC Addr Protocol Description
11 9.327851 LOCAL 000C29022861 ISAKMP Major Version: 1 Minor Version: 0 Length: 52
12 9.327851 000C29022861 LOCAL ISAKMP Major Version: 1 Minor Version: 0 Length: 84
13 9.343476 LOCAL 000C29022861 ESP SPI = 0x202A4421, Seq = 0x1
14 9.359101 000C29022861 LOCAL ESP SPI = 0x5FFB6BF5, Seq = 0x1

Bước 11: Chọn ESP: nhận xét thấy dữ liệu trên đường truyền đã được mã hóa

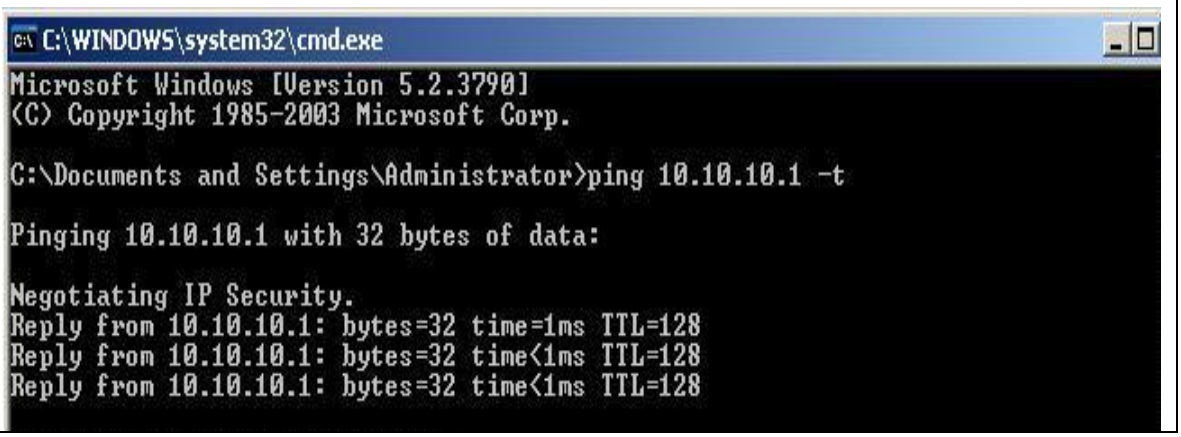

Microsoft Network Monitor - [Capture: 1 (Detail)]
File Edit Display Tools Options Window Help
Frame Time Src MAC Addr Dst MAC Addr Protocol Description
13 9.343476 LOCAL 000C29022861 ESP SPI = 0x202A4421, Seq = 0x1
14 9.359101 000C29022861 LOCAL ESP SPI = 0x5FFB6BF5, Seq = 0x1
ESP: SPI = 0x202A4421, Seq = 0x1
ESP: Security Parameters Index = 539640865 (0x202A4421)
ESP: Sequence Number = 1 (0x1)
ESP: Rest of Frame (encrypted): Number of data bytes remaining = 68 (0x0044)
00000000 00 0C 29 02 28 61 00 0C 29 C7 4B EF 08 00 45 00
00000010 00 60 01 9B 00 00 80 32 10 BB 0A 0A 0A 02 0A 0A
00000020 0A 01 20 2A 44 21 00 00 00 01 F2 A6 23 F4 C0 85
00000030 7C 1C C3 AF 91 59 C0 30 86 14 C7 86 FB 55 1A E2
00000040 50 F7 2E 6D 4C AC 35 0B 37 B1 C2 28 F4 93 76 1C
Summary of the ESP Packet
F#: 13/37
Off: 34 (x22)

Bước 12: Trên server2 ping địa chỉa IP của server3 , nhận thấy đường truyền

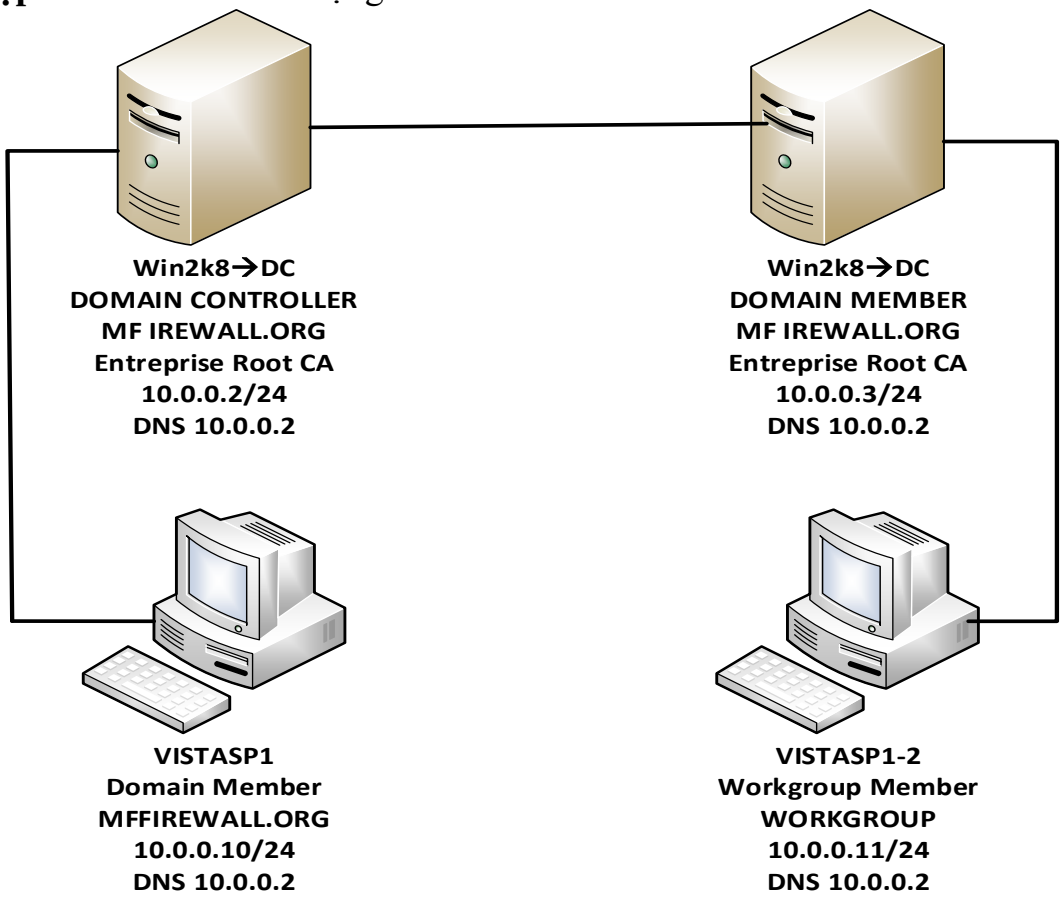
không liên lạc được với nhau


C:\WINDOWS\system32\cmd.exe - ping 10.10.10.3 -t
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
C:\Documents and Settings\Administrator>ping 10.10.10.3 -t
Pinging 10.10.10.3 with 32 bytes of data:
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.

Bước 13: Server2 ping địa chỉ IP của Server1 với tham số -t, thấy hệ thống báo Negotiating IP Security và đường truyền thông


C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
C:\Documents and Settings\Administrator>ping 10.10.10.1 -t
Pinging 10.10.10.1 with 32 bytes of data:
Negotiating IP Security.
Reply from 10.10.10.1: bytes=32 time=1ms TTL=128
Reply from 10.10.10.1: bytes=32 time<1ms TTL=128
Reply from 10.10.10.1: bytes=32 time<1ms TTL=128

Bài tập 3 : cho mô hình mạng như sau:



Yêu cầu: Triển khai IPsec Server và Domain Isolation bằng Windows Server 2008 Group Policy

Chuẩn bị:

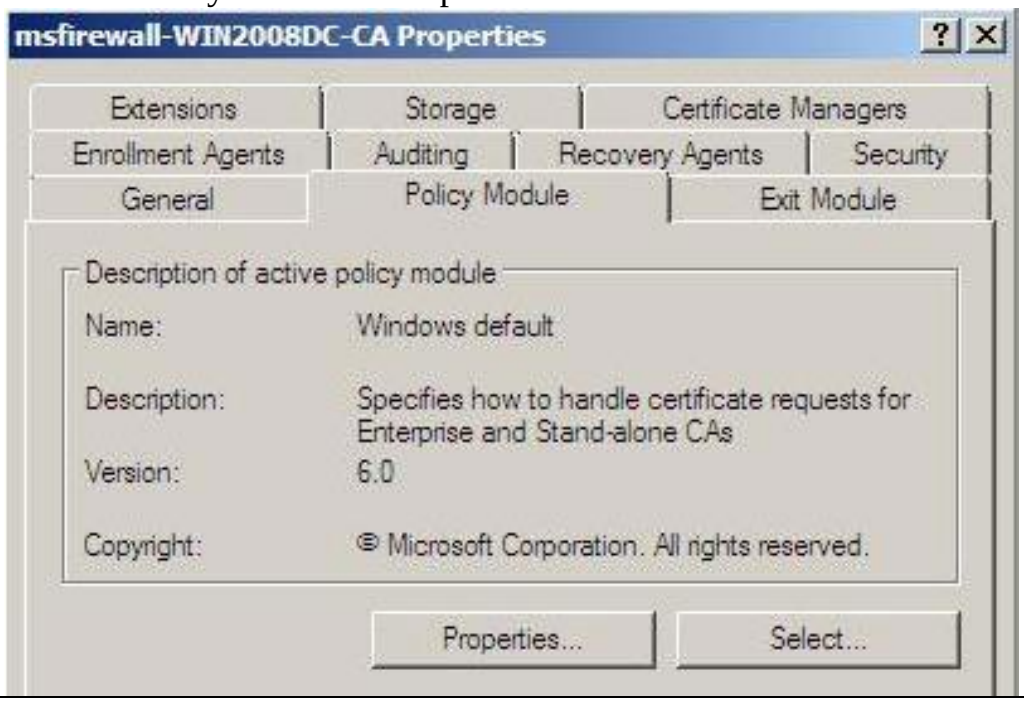
- 1 máy PC cài win 2k8→ msfirewall-WIN2008DC-CA.
- 1 máy PC cài win 2k8→ WIN2008SRV1
- 1 máy PC cài win vista→ VISTASP1 msfirewall.org.
- 1 máy PC cài win vista→VISTASP1-2 WORKGROUP

Thực hiện

1.Xác nhận cấu hình Enterprise Root CA trên bộ điều khiển miền

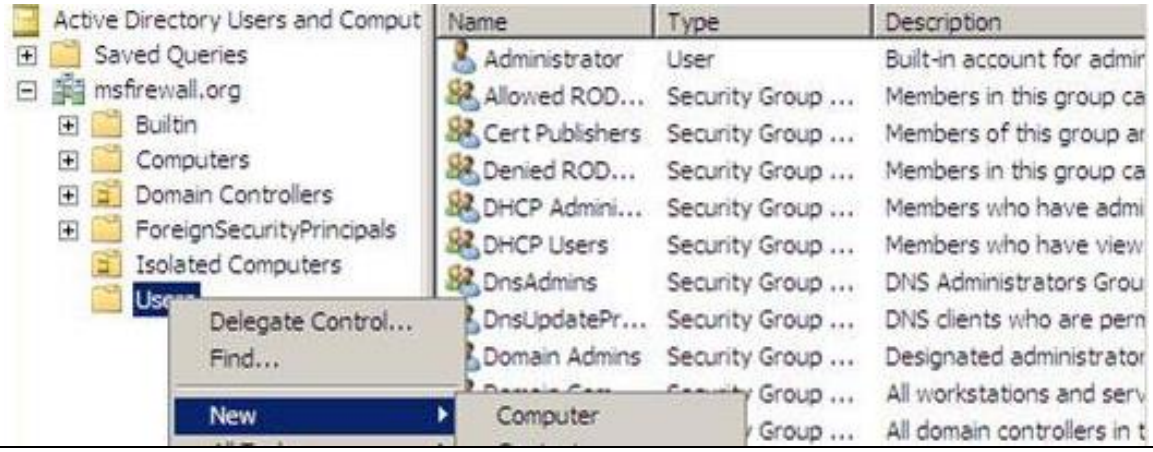
Bước 1: Start→Administrative Tools →Certification Authority → CA→ Properties

Bước 2: Tab Policy Module→Properties

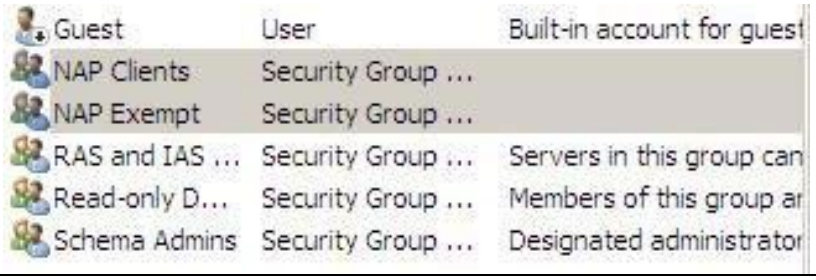


2.Tạo nhóm NAP CLIENTS

Bước 1: Active Directory Users and Computers→ msfirewall.org**,** →New → Group

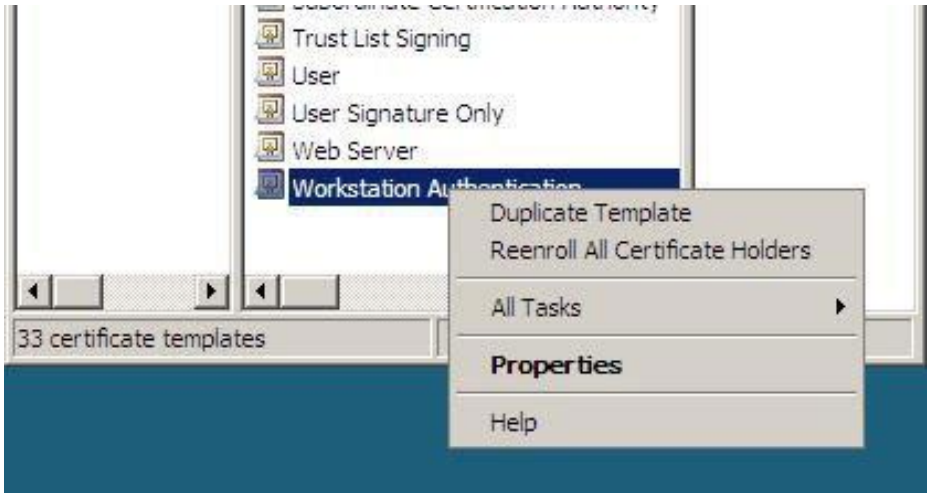


Bước 2: Giao diện điều khiển Active Directory Users and Computers



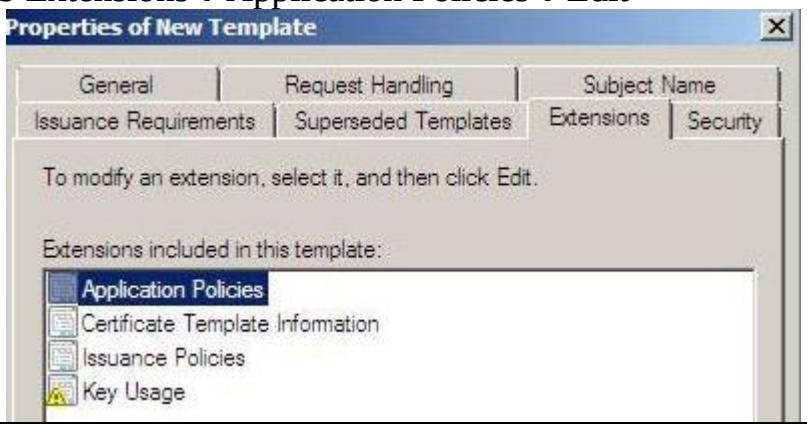
3.Tạo và cấu hình mẫu chứng chỉ cho NAP Exempt Computer

Bước 1: WIN2008DC→Start→Run -> certtmpl.msc → ENTER →Certificate Template Console→ Workstation Authentication →Duplicate Template.

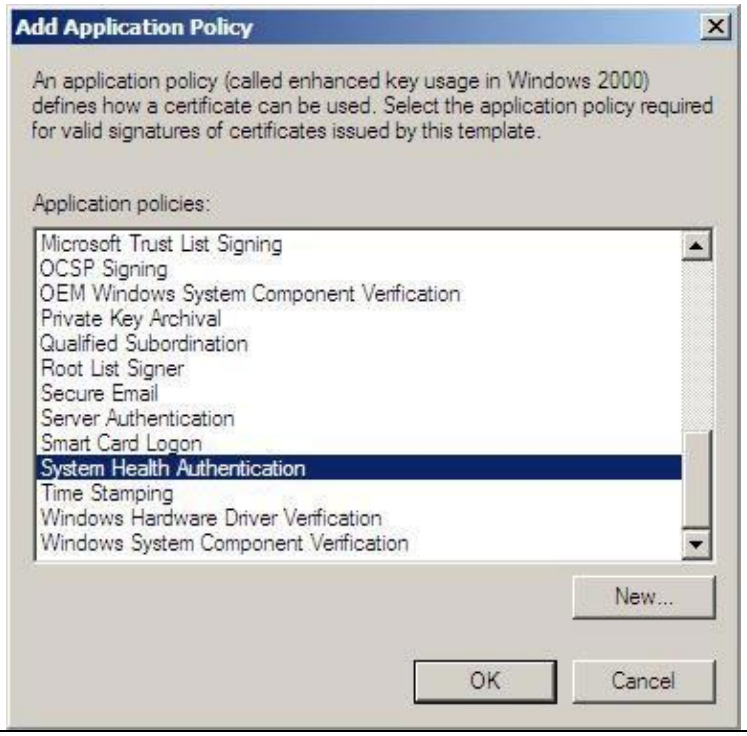


Bước 2: Duplicate Template→ Windows 2003 Server→ OK→ Template display name→System Health Authentication→Publish certificate in Active Directory.

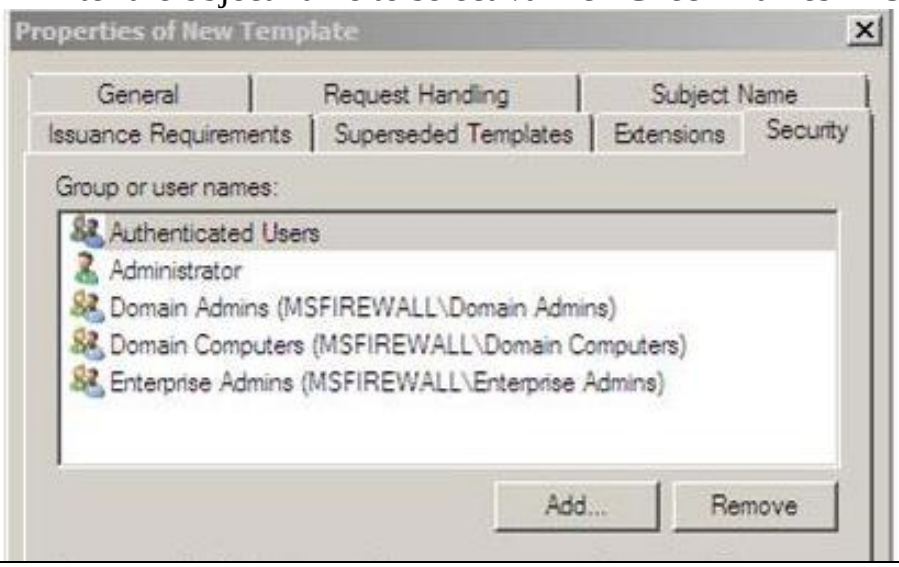
Bước 3: Tab Extensions→Application Policies→Edit



Bước 4: Edit Application Policies Extension→ Add→ Add Application Policy→System Health Authentication → OK.


Add Application Policy
An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.
Application policies:
Microsoft Trust List Signing
OCSP Signing
OEM Windows System Component Verification
Private Key Archival
Qualified Subordination
Root List Signer
Secure Email
Server Authentication
Smart Card Logon
System Health Authentication
Time Stamping
Windows Hardware Driver Verification
Windows System Component Verification
New...
OK
Cancel

Bước 5: Tab Security → Add→Select Users, Computers or Groups→ NAP Exempt → Enter the object name to select và kích Check Names→ OK.



4.Làm cho mẫu chứng chỉ hiện hữu cho việc công bố trong Group Policy

Bước 1: WIN2008DC→ Start→Run đánh certsrv.msc → ENTER→ Certificate Templates→New→Certificate Template to Issue.

Bước 2: System Health Authentication→ OK

Enable Certificate Templates
Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.
Name
Intended Purpose
OCSP Response Signing
OCSP Signing
RAS and IAS Server
Client Authentication, Server Authentication
Router (Offline request)
Client Authentication
Smartcard Logon
Client Authentication, Smart Card Logon
Smartcard User
Secure Email, Client Authentication, Smart Card Logon
System Health Authentication
System Health Authentication, Client Authentication
Trust List Signing
Microsoft Trust List Signing
User Signature Only
Secure Email, Client Authentication
Workstation Authentication
Client Authentication
OK
Cancel

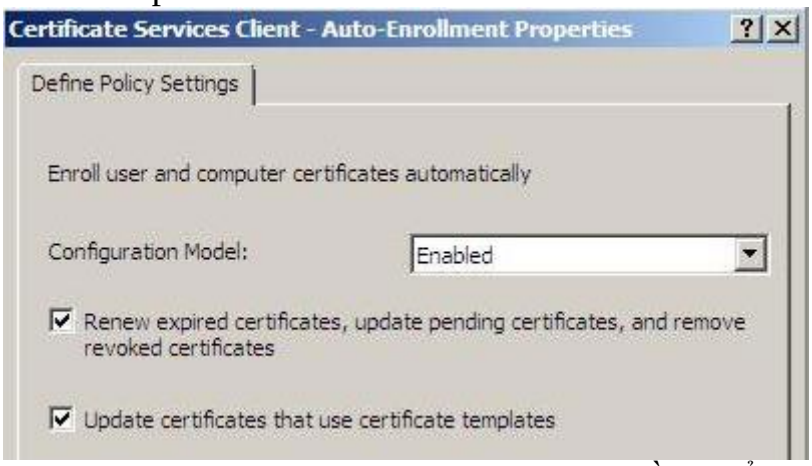
Bước 3: Trong panel bên trái của giao diện điều khiển→Certificate Templates, trong phần panel chi tiết nằm trong phần Name, hãy thẩm định rằng System Health Authentication đã được hiển thị.

5.Phân phối chứng chỉ sức khỏe NAP Exemption trong Group Policy Autoenrollment

Bước 1: Start → kích Run→ gpmc.msc → Open→OK→Group Policy Management→ msfirewall.org → Default Domain Policy → Edit.

Bước 2: Group Policy Management Editor→Computer Configuration\Windows Settings\Security Settings\Public Key Policies.
→ Certificate Services Client – Auto-Enrollment.

Bước 3: Certificate Services Client – Auto-Enrollment Properties→Configuration Model. → Renew Expired certificates, update pending certificates, and remove revoked certificates và Update certificates that use certificate templates→OK


Certificate Services Client - Auto-Enrollment Properties
Define Policy Settings
Enroll user and computer certificates automatically
Configuration Model:
Enabled
Renew expired certificates, update pending certificates, and remove revoked certificates
Update certificates that use certificate templates

Group Policy Management Editor →Đóng giao diện điều khiển Group Policy Management

5. TÓM TẮT NỘI DUNG

- Khái niệm mã hóa, tại sao cần mã hóa thông tin.
- Khái niệm mã hóa đối xứng, cơ chế, các thành phần của hệ mã hóa đối xứng.
- Các kiểu tấn công hệ mã hóa đối xứng (ciphertext only, known plaintext, chosen plaintext, chosen ciphertext).
- Khái niệm mã hóa bất đối xứng, cơ chế, các thành phần của hệ mã hóa bất đối xứng.
- Các đặc điểm và yêu cầu của hệ mã hóa bất đối xứng.
- Chứng thực bằng mã hóa đối xứng và mã hóa bất đối xứng

6. CÂU HỎI VÀ BÀI TẬP

CÂU HỎI

Câu 1: IP Security là gì?

Câu 2: Trình bày. khái niệm mã hóa, tại sao cần mã hóa thông tin ?

Câu 3: Trình bày khái niệm mã hóa đối xứng, cơ chế, các thành phần của hệ mã hóa đối xứng**.**

Câu 4: Trình bày Các kiểu tấn công hệ mã hóa đối xứng (ciphertext only, known plaintext, chosen plaintext, chosen ciphertext).

Câu 5:Nêu quá trình quản lý và kiểm soát truy cập từ xa bằng IPSec VPN.

BÀI TẬP

Bài tập 1: Bảo mật website với SSL certificate của VeriSign.com

Yêu cầu: Cài đặt, cấu hình cơ chế mã hóa của SSL:

Chuẩn bị

- Máy Windows Server 2008
- Cài đặt dịch vụ Internet Information Services (IIS)
- Hosting Web Site
- 1 switch
- 1 router kết nối internet
- 2 sợi cáp bấm thẳng

Hướng dẫn làm bài

1.Tạo Request Certificate

B1:Logon Administrator, mở Internet Information Services (IIS) Manager, bung Web Site, chuột phải Default Web Site, chọn Properties

B2:Hộp thoại Default Web Site Properties, qua tab Directory Security, chọn Server Certificate

B3:Hộp thoại Welcome to the Web Server Certificate Wizard, chọn Next

B4: Hộp thoại Server Certificate, chọn Create anew certificate, chọn Next

B5: Trong hộp thoại Delayed or Immediate Request, chọn Prepare the request now, but send it later, chọn Next

B6: Hộp thoại Name and Security Settings, chọn Next

B7: rong hộp thoại Organization Information, nhập thông tin, chọn Next

B8: Nhập thông tin trang web, đường dẫn chứa trang webchọn Finish

2. Xin SSL Certificate từ VeriSign.com

B1:Mở Windows Explorer, copy nội dụng của file C:\certreq.txt

B2: Mở Internet Explorer, truy cập địa chỉ http://www.verisign.com, chọn Free SSL Trial

B3: Trong cửa sổ Free SSL Trial Certificate, nhập đầy đủ thông tin (*: thông tin bắt buộc), chọn Continue

B4: Cửa sổ Welcome, chọn Continue

B5: Cửa sổ tiếp theo, nhập đầy đủ thông tin vào phần Technical Contact, chọn Continue

B6: Trong ô Select Server Platform, chọn Microsoft. Trong ô Select Version, chọn IIS 6.0. Dán nội dung file certreq.txt vào ô Paste Certificate Signing Request (CSR), optained from your server

B7: Trong ô What do you plan to use this SSL Certificate for?, chọn Web Server, chọn Continue

B8: Trong cửa sổ CRS Information, nhập MSOPENLAB vào ô Challenge Phrase và Re-enter Challenge Phrase. Nhập câu hỏi bất kỳ vào ô Reminder Question, chọn Continue

B9: Trong cửa sổ Order summary & acceptance, chọn Accept

B10: Kiểm tra: xin SSL Certificate thành công

3. Cấu hình Trusted Root Certification Authority

B1:Đăng nhập vào hộp mail, kiểm tra nhận được e-mail từ Support@verisign.com

B2: Trong trang web của verisign, chọn VeriSign CA Certificates

B3: Chọn Secure Site Trial Root CA Certificate

B4: Trong cửa sổ Root CA Certificate, chọn Select All, copy tất cả nội dung

B5: Dán nội dung vào Notepad và save lại với tên ca.cer

B6: Mở Internet Explorer, vào Tools, chọn Internet Options, qua tab Content, chọn Certificates

B7: Trong hộp thoại Certificates, chọn Import

B8: Hộp thoại Welcome to the Certificate Import Wizard, chọn Next

B9: Hộp thoại File to Import, chọn Browse, trỏ đường dẫn đến C:\ca.cer, chọn Next

B10:Hộp thoại Security Warning, chọn Yes

4. Import SSL Certificate cho Web Server

B1:Đăng nhập vào hộp mail, mở e-mail của support@verisign.com, copy phần BEGIN CERTIFICATE

B2:Dán nội dung vào Notepad, save lại với tên cert.txt

B3: Mở Internet Information Services (IIS) Manager, chuột phải Default Web Site chọn Properties. Trong cửa sổ Default Web Site Properties, qua tab Directory Security, chọn Server Certificate

B4: Hộp thoại Pending Certificate Request, chọn Process the pending request and install the certificate, chọn Next

B5: Hộp thoại Process a Pending Request, chọn Browse, trỏ đường dẫn đến C:\cert.txt

B6: Hộp thoại SSL Port, giữ mặc định port 443, chọn Next 2 lần, chọn Finish

B7: Trong hộp thoại Default Web Site Properties, chọn View Certificate

B8: Kiểm tra Certificate được cấp bởi Verisign

B9:Kiểm tra kết quả. Mở Internet Explorer, truy cập https://www.MSOpenLab.com, kiểm tra truy cập thành công

Bài tập 2: Cài đặt, cấu hình BitLocker Drive Encryption

Yêu cầu: Thực hiện mã hóa ổ đĩa và bảo mật dữ liệu trên win2k8

Chuẩn bị

- 1 máy PC cài đặt win2k8
- 1 USB để lưu trữ key giải mã

Hướng dẫn làm bài

1. Chia partition khi cài Windows Server 2008

B1: Khởi động máy tính bằng đĩa cài đặt Windows Server 2008

B2: Trong màn hình Install Windows→ Language, Time and currency format, và Keyboard Layout→Next

B3: Trong hộp thoại tiếp theo→Repair your computer→Next→Command Prompt

2. Cài đặt BitLocker Drive Encryption

B1: Chuột phải lên Features, chọn Add Features

B2: Trong hộp thoại Select Features, đánh dấu →BitLocker Drive Encryption

B3: Trong hộp thoại Confirmation→ Install để bắt đầu quá trình cài đặt

B4: Sau khi cài đặt xong, bạn Restart lại máy

3. Mở tính năng BitLocker Drive Encryption trên máy không có chip TPM

B1:Vào Start\Run, gõ: gpedit.msc

B2: Trong console Local Group Policy Editor→Computer Configuration, bung dấu cộng của Administrative Templates→Windows Components→BitLocker Drive Encryp

B3: Chuột phải vào Control Panel Setup: Enable Advanced Startup Options →Properties →Enable→check vào tùy chọn Allo

B4: BitLocker without a compatible TPM→OK→ Start\Run, gõ gpupdate /force

B5:Mở Control Panel→mục Security→ BitLocker Drive Encryption

B6: Trong trang BitLocker Drive Encrytion→Turn On BitLocker

B7: Trong mục Set BitLocker startup preferences→Require Startup USB key at every startup

B8: gắn USB vào máy→ USB→ Save

- Trong mục Save the recovery password, bạn sẽ thấy các tùy chọn sau:

- Save the password on a USB drive : lưu mật khẩu trên ổ dĩa USB
- Save the password in a folder: lưu mật khẩu vào thư mục trên ổ đĩa mạng
- Print the password: in mật khẩu

Bài tập 3: Administrator sẽ mã hóa tất cả các dữ liệu được đặt trong folder mã hóa theo từng phòng ban

- Mỗi phòng ban sẽ có 1 thư mục dùng để mã hóa → User muốn mã hóa dữ liệu nào phải copy qua thư mục riêng (ex: WILLBE_ENCRYPT) → Admin sẽ copy dữ liệu này vào thư mục mã hóa tương ứng theo từng phòng ban
- Sau đó admin sẽ chạy lại lệnh add user được quyền read/write trên thư mục đã mã hóa.

Yêu cầu:

- Mã hóa những dữ liệu quan trọng cho từng phòng ban
- Dữ liệu mã hóa khi đem ra ngoài hệ thống (không được chứng thực CA + Domain) →không thể mở

Chuẩn bị :

- File Server chạy Windows Server 2012: share file/folder theo chuẩn SMB (SMB mình sẽ có 1 bài riêng cho nó).
- Máy Domain + CA chạy Windows Server 2012
- Máy Client chạy Windows 7 Pro
- Tài khoản Administrator (ivim.admin), 2 Tài khoản user để kiểm tra kết quả (ivim.test05 và ivim.test06)

Hướng dẫn làm bài

B1. Log on bằng user(người dùng) trên fileserver → tạo chữ ký số theo mẫu EFS base → Dùng lệnh export chữ ký số.

B2. Log out khoỉ user người dùng và log on bằng user admin → Tạo thư mục phân quyền và tạo chế độ mã hóa → Add user được quyền read/write.

B3. Import chữ ký số pfx (computer name + user name →) vào PC người dùng

B4. Test người dùng log on bằng máy của mình → có thể mở được dữ liệu đã mã hóa

- Người dùng mã hóa EFS trên máy cá nhân(máy đã join domain) → Sẽ phát sinh trên CA chữ ký số EFS khác → chỉ có thể phân biệt bằng thumbprint trên từng chữ ký số, trong trường hợp này không thể dùng lệnh add user theo user name→Phải adduser bằng hash khi có nhiều chữ ký số EFS cho một user → đảm bảo khớp chữ ký số mã hóa phát sinh từ fileserver

BÀI 3: NETWORK ADDRESS TRANSLATION

viết tắt NAT

Mã bài MĐ 26-03

Thời gian :8 giờ

I. MỤC TIÊU: Sau khi học bài học này, sinh viên có khả năng

- Trình bày được quá trình NAT của một hệ thống mạng ;
- Trình bày được NAT tĩnh và NAT động ;
- Thiết lập cấu hình NAT trên Windows server.
- Thực hiện các thao tác an toàn với máy tính

II. NỘI DUNG CHÍNH

1. Giới thiệu

Mục tiêu: Trình bày được quá trình NAT của một hệ thống mạng

Kỹ thuật NAT (Network Address Translation): là một kỹ thuật được phát minh lúc khởi đầu dùng để giải quyết vấn đề IP shortage. Khi có hai máy tính ở trên cùng một lớp mạng (cùng subnet), các máy tính này kết nối trực tiếp với nhau, điều này có nghĩa là chúng có thể gởi và nhận dữ liệu trực tiếp với nhau. Nếu những máy tính này không trên cùng một lớp mạng và không có kết nối trực tiếp thì dữ liệu sẽ được chuyển tiếp qua lại giữa những lớp mạng này và như thế phải cần một router (có thể là phần mềm hoặc phần cứng) Đây là trường hợp khi một máy tính nào đó muốn kết nối tới một máy khác trên internet.

2. Các kỹ thuật Nat cổ điển

*Mục tiêu***:** *Trình bày được NAT tĩnh và NAT động*

2.1 NAT tĩnh

Với NAT tĩnh thì sự chuyển đổi gói tin giữa hai mạng, giữa nguồn và địa chỉ đến trở nên đơn giản và nhất định. NAT cố định được thiết kế để ánh xạ một-một, từ một địa chỉ nội bộ sang một địa chỉ công cộng tương ứng duy nhất.

Bên ngoài (outside) có thể chủ động tạo kết nối với bên trong (inside). Cơ chế NAT tĩnh cho phép một máy chủ bên trong hiện diện ra ngoài Internet, bởi vì máy chủ sẽ luôn dùng cùng một địa chỉ IP thực .

2.2 NAT động

NAT động được thiết kế để ánh xạ một địa chỉ IP riêng sang một địa chỉ công cộng một cách tự động. Bất kỳ địa chỉ IP nào nằm trong dải địa chỉ IP công cộng đã được định trước đều có thể được gán cho một host bên trong mạng.

3. NAT trong Windows server

Mục tiêu:Thiết lập cấu hình NAT trên Windows server

Nguyên Lý Hoạt Động Của NAT:

NAT làm việc như một router, công việc của nó là chuyển tiếp các gói tin (packets) giữa những lớp mạng khác nhau trên một mạng lớn. Bạn cũng có thể nghĩ rằng Internet là một mạng đơn nhưng có vô số subnet. Routers có đủ khả năng để hiểu được các lớp mạng khác nhau xung quanh nó và có thể chuyển tiếp những gói tin đến đúng nơi cần đến.

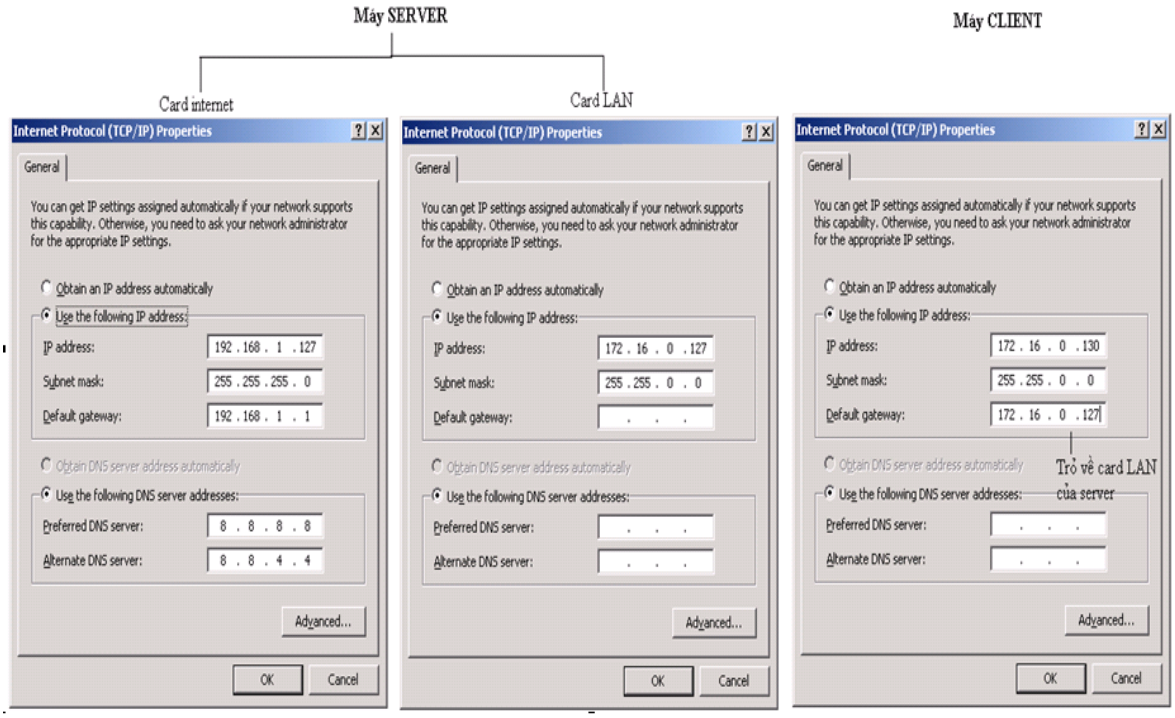
NAT sử dụng IP của chính nó làm IP công cộng cho mỗi máy con (client) với IP riêng. Khi một máy con thực hiện kết nối hoặc gởi dữ liệu tới một máy tính nào đó trên internet, dữ liệu sẽ được gởi tới NAT, sau đó NAT sẽ thay thế địa chỉ IP gốc của máy con đó rồi gửi gói dữ liệu đi với địa chỉ IP của NAT. Máy tính từ xa hoặc máy tính nào đó trên internet khi nhận được tín hiệu sẽ gởi gói tin trở về cho NAT computer bởi vì chúng nghĩ rằng NAT computer là máy đã gởi những gói dữ liệu đi. NAT ghi lại bảng thông tin của những máy tính đã gởi những gói tin đi ra ngoài trên mỗi cổng dịch vụ và gởi những gói tin nhận được về đúng máy tính đó (client).

4.Bài tập thực hành

Bài tập 1: Triển khai dịch vụ NAT

Chuẩn bị

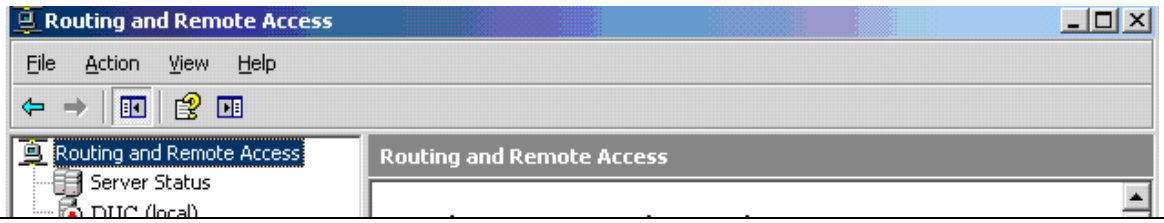
- 1 máy PC cài winXP
- 1 máy PC cài win2k3, có 2 card mạng Card Internet Nối với Ruoter và Card LAN nối với máy Client
- Thiết lập địa chỉ IP cho 2 máy


Máy SERVER
Máy CLIENT
Card internet
Card LAN
Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 127
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 8 . 8 . 8 . 8
Alternate DNS server: 8 . 8 . 4 . 4
Advanced...
OK
Cancel
Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 172 . 16 . 0 . 127
Subnet mask: 255 . 255 . 0 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel
Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 172 . 16 . 0 . 130
Subnet mask: 255 . 255 . 0 . 0
Default gateway: 172 . 16 . 0 . 127
Trỏ về card LAN của server
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

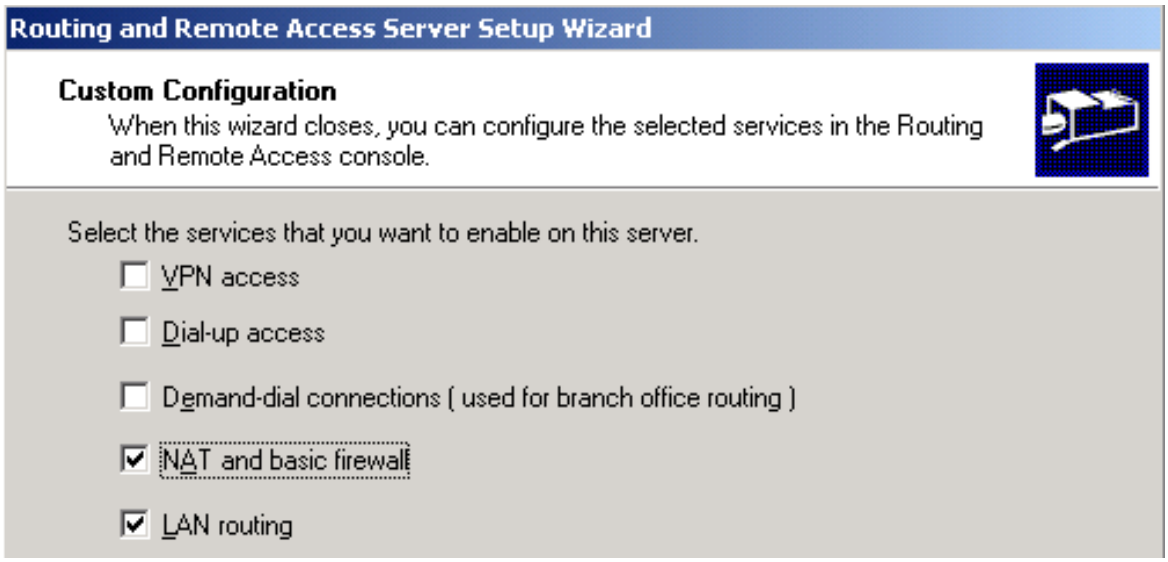
Thực hiện

Các bước cài đặt

Bước 1: Routing and Remote Access→ R_Click chuột vào Tên Server chọn Configure and Enable Routing and Remote Access→Next



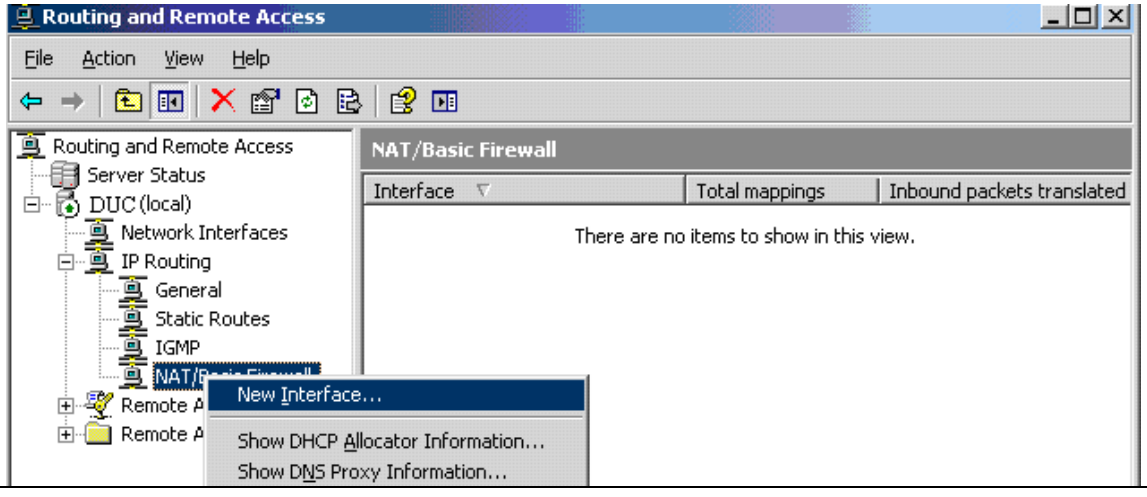
Bước 2: Nhấp chọn Custom configuration→Next→check NAT…LAN..-->Next


Routing and Remote Access Server Setup Wizard
Custom Configuration
When this wizard closes, you can configure the selected services in the Routing and Remote Access console.
Select the services that you want to enable on this server.
VPN access
Dial-up access
Demand-dial connections (used for branch office routing)
NAT and basic firewall
LAN routing

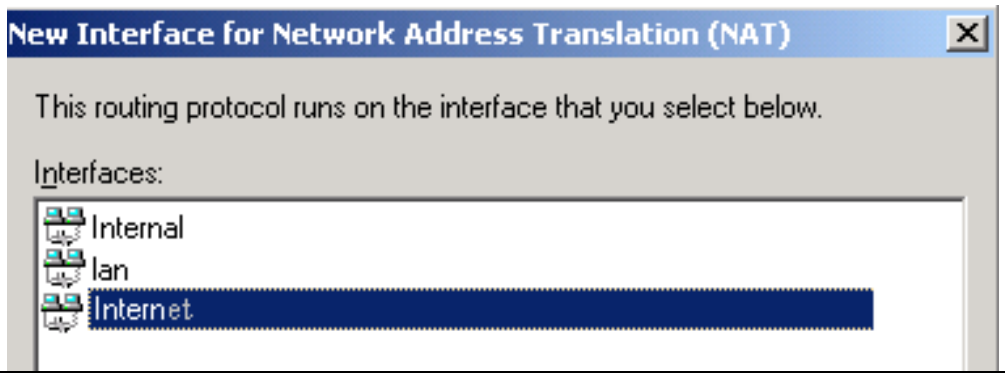
Kế tiếp→ Finish→Yes

Cấu hình

Bước 1: mở IP Routing/R_Click chọn NAT/Basic Firewall → New Interface…

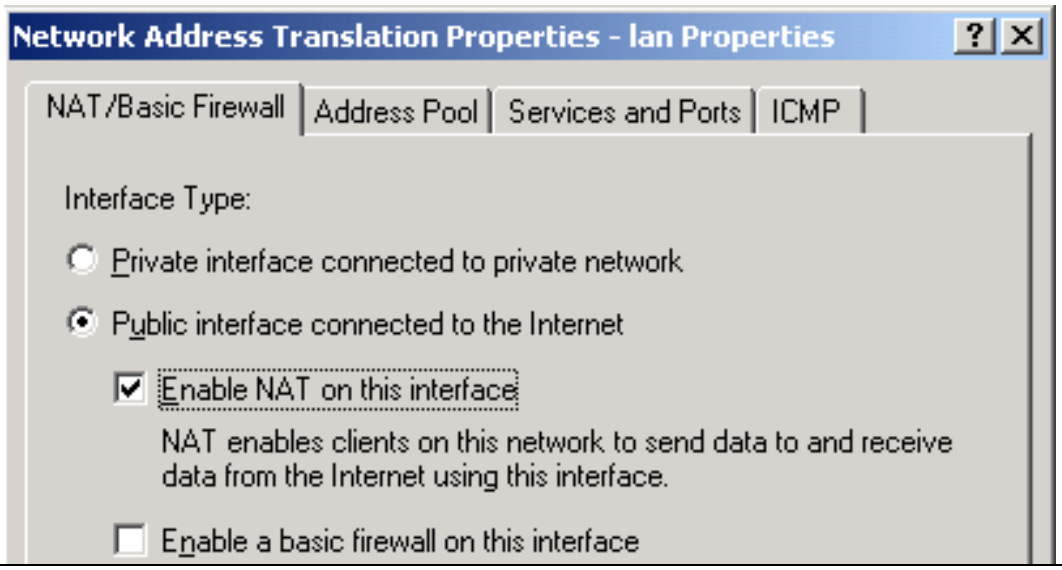


Bước 2: Chọn Internet – Ok

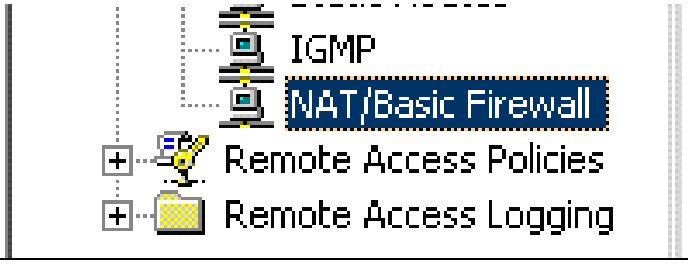


Bước 3: Chọn vào Mục: Pucblic interface connected to the internet

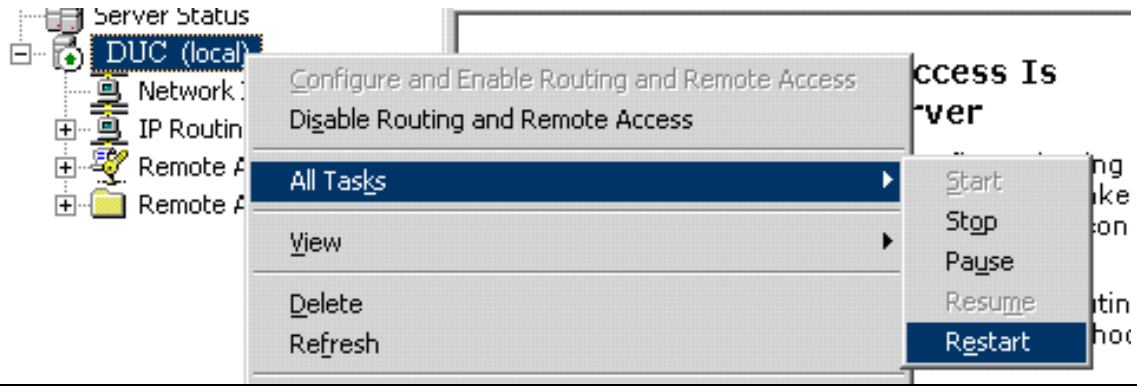
Check vào ô: Enable NAT on This interface →Apply →OK


Network Address Translation Properties - lan Properties
NAT/Basic Firewall
Address Pool
Services and Ports
ICMP
Interface Type:
Private interface connected to private network
Public interface connected to the Internet
Enable NAT on this interface
NAT enables clients on this network to send data to and receive data from the Internet using this interface.
Enable a basic firewall on this interface

Bước 4: Tiếp theo R_click NAT/Basic Firewall → New Interface→OK



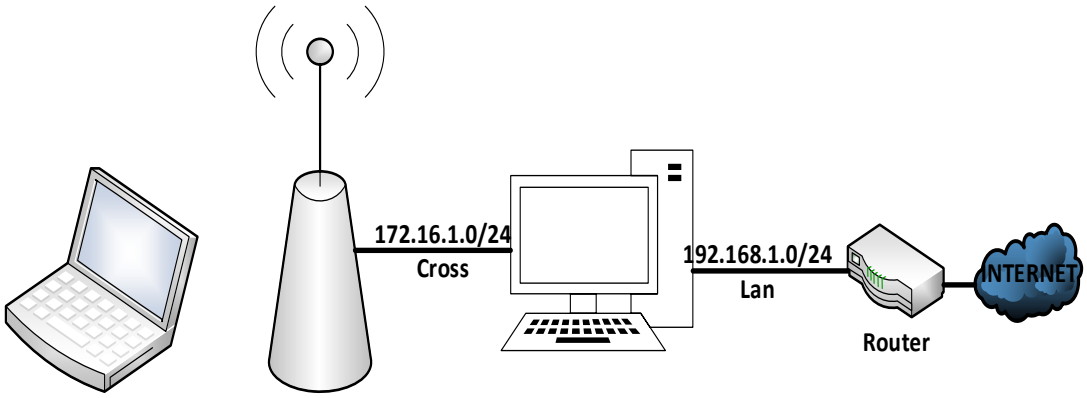
Bước 5: Kế tiếp R_Click Tên server(DUC)→All Tasks→Restart



Bước 6: máy Client vào **Internet Explorer** gõ vào địa chỉ www.google.com.vn

Google - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.google.com.vn/
Go Links
Web Hình ảnh Video Tin tức Dịch Giải Đáp Gmail thêm
iGoogle | Cài đặt tìm kiếm | Đăng nhập
Google
Việt Nam
Tìm kiếm nâng cao
Công cụ ngôn ngữ
Tìm với Google
Xem trang đầu tiên tìm được
Tìm kiếm trên: web những trang viết bằng tiếng Việt những trang từ Việt Nam

Bài tập 2: Cho mô hình mạng như sau**:**



Yêu cầu: Thực hiện quản lý kết nối Internet không dây với Wireless Gateway Antamedia

Chuẩn bị:

- Một đường truyền ADSL
- Mọt Router ADSL đã được cấu hình kết nối Internet
- Một Wireless Access Point
- Một máy tính có 2 Card mạng làm Wireless Gateway
- Một máy tính Client có tích hợp Card mạng Wireless

Thiết lập địa chỉ IP

Máy PC15 (Wireless gateway)

Card LAN (kết nối với Router ADSL để truy cập Internet)

- IP Address: 192.168.1.15
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.188.1.1 (địa chỉ Router ADSL)
- Prefered DNS Server: 210.245.24.20

Card CROSS (kết nối với Wireless Access Point)

- IP Address: 172.16.1.15
- Subnet Mask: 255.255.255.0
- Default Gateway: (để trống)
- Prefered DNS Server: (để trống)

Máy Client để chế độ nhận IP động

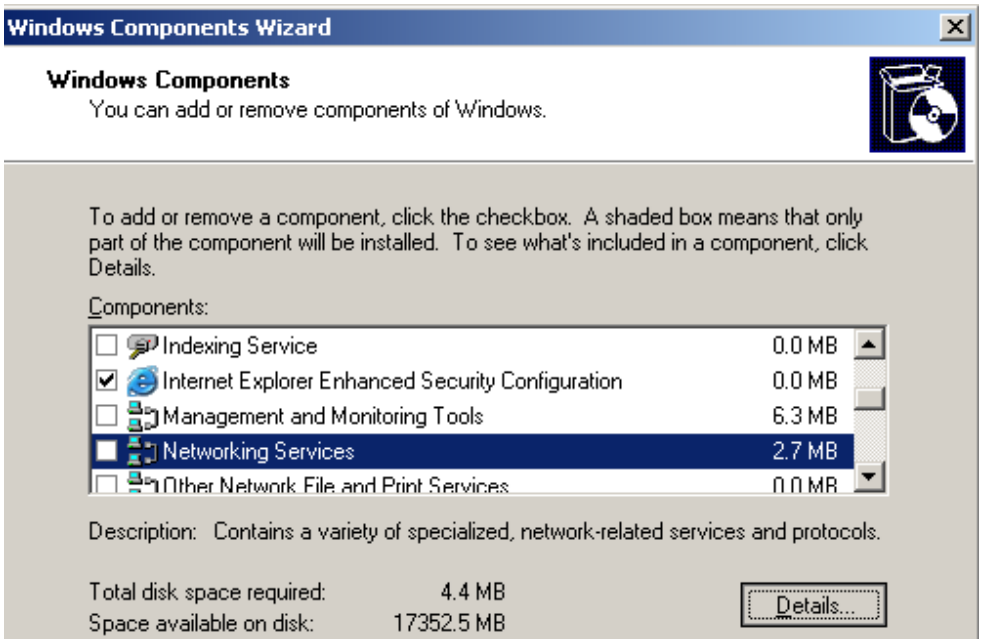
Thực hiện

Các bước cài đặt

4.1 Cấu hình NAT Outbound trên PC15 (xem bài tập trên)

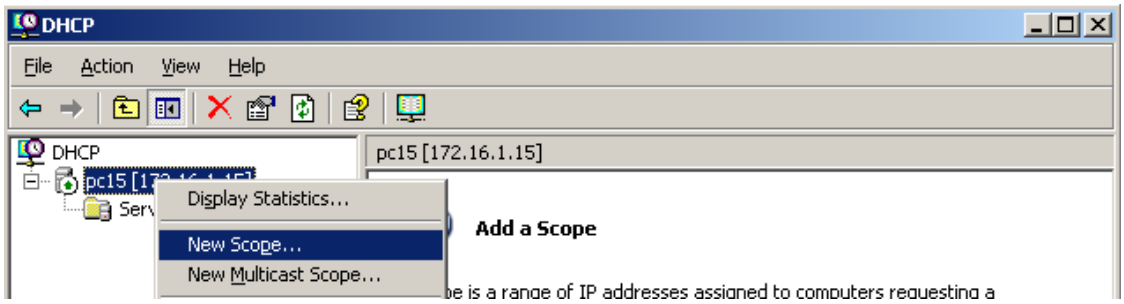
4.2 Cài đặt và cấu hình DHCP trên PC15

Bước 1: Mở Control Panel →Add or Remove Programs -- Add/Remove Windows Components


Windows Components Wizard
Windows Components
You can add or remove components of Windows.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Indexing Service 0.0 MB
Internet Explorer Enhanced Security Configuration 0.0 MB
Management and Monitoring Tools 6.3 MB
Networking Services 2.7 MB
Other Network File and Print Services 0.0 MB
Description: Contains a variety of specialized, network-related services and protocols.
Total disk space required: 4.4 MB
Space available on disk: 17352.5 MB
Details...

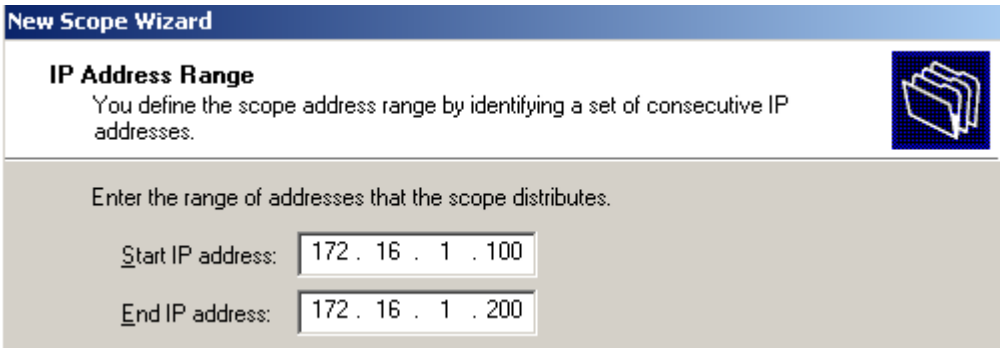
Chọn Networking Service → Nhấn Detail→ Đánh dấu chọn Dynamic Host Configuration Protocol (DHCP)→OK→Next

Bước 2: trên DHCP Server, tạo 1 Scope để cấp IP cho các máy Client→Next



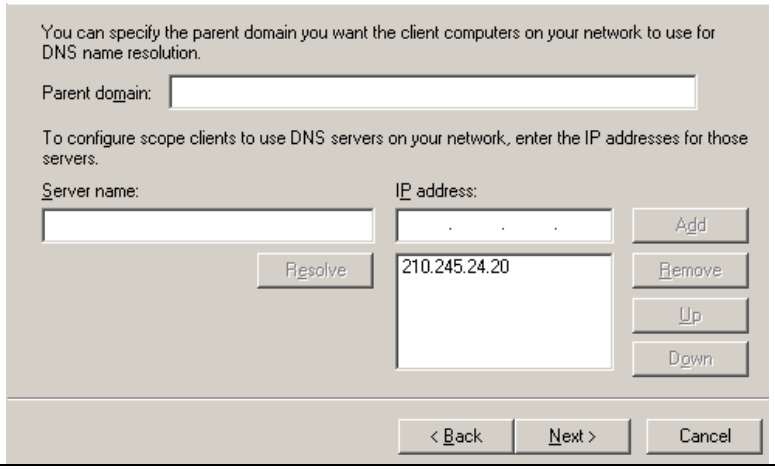
Kế tiếp →đặt tên Scope→Next

Bước 3: Nhập địa chỉ IP →Next→Next→Next


New Scope Wizard
IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.
Enter the range of addresses that the scope distributes.
Start IP address:
172 . 16 . 1 . 100
End IP address:
172 . 16 . 1 . 200

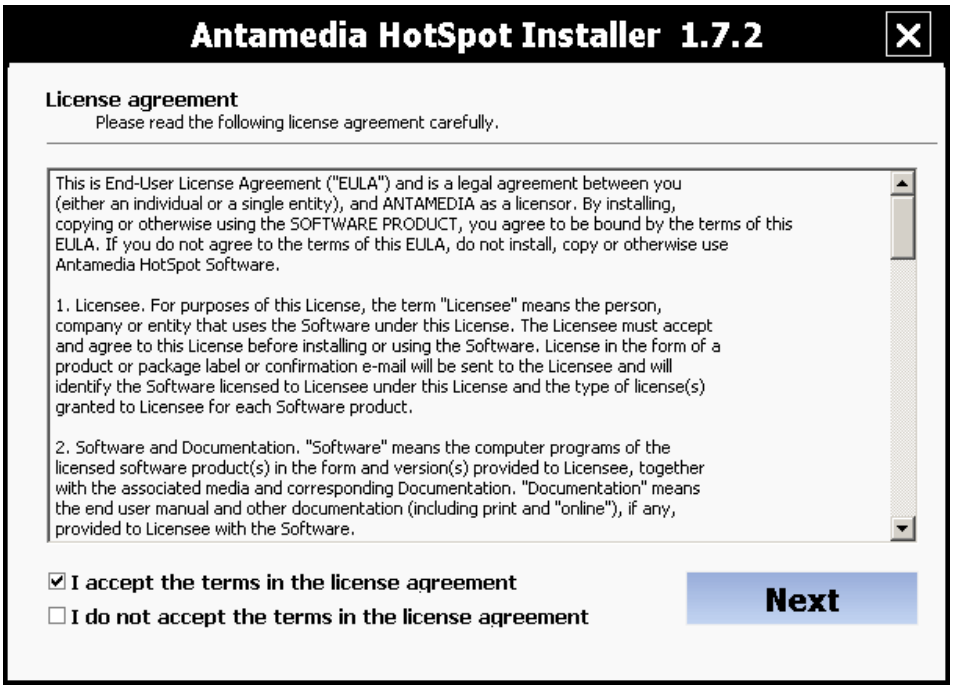
Chọn yes…→Next→ Nhập địa chỉ default→Next

Bước 4: Nhập địa DNS→Next→Next→ Finsh


You can specify the parent domain you want the client computers on your network to use for DNS name resolution.
Parent domain:
To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.
Server name:
IP address:
Add
Resolve
210.245.24.20
Remove
Up
Down
< Back
Next >
Cancel

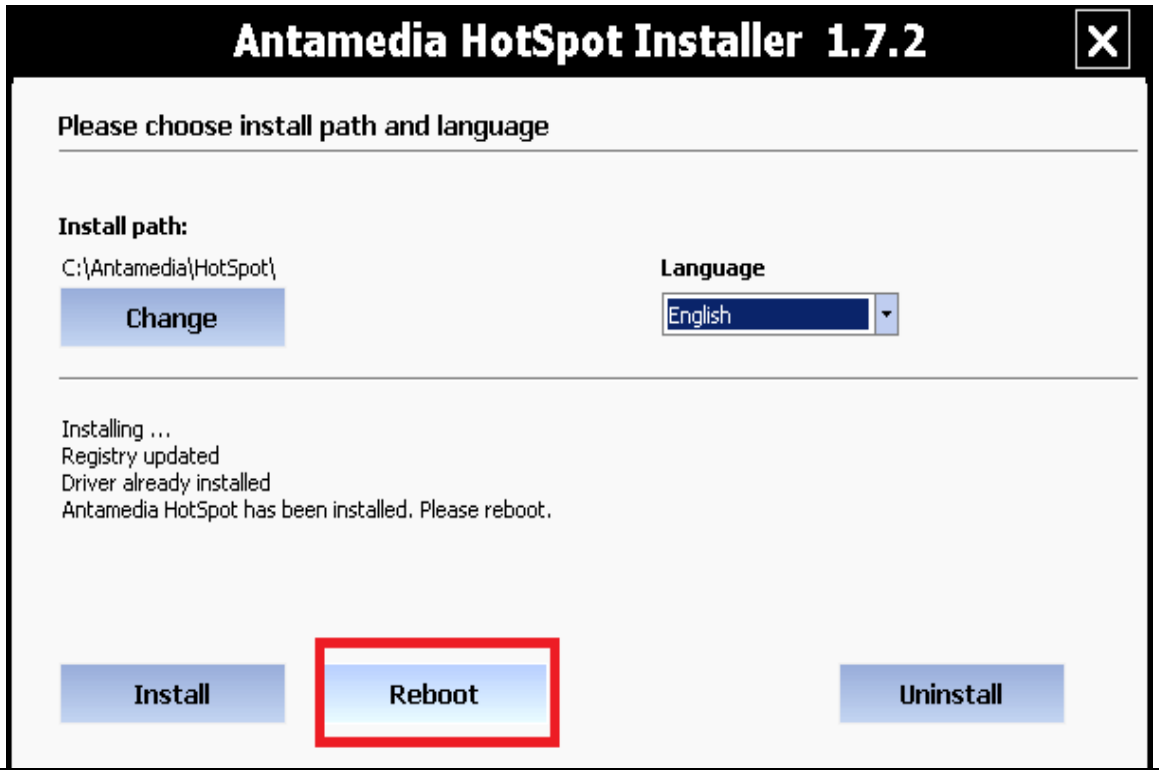
4.3 Cài đặt Antamedia

Bước 1: Chạy File chương trình cài đặt→ Đồng ý các thông tin bản quyền→Next

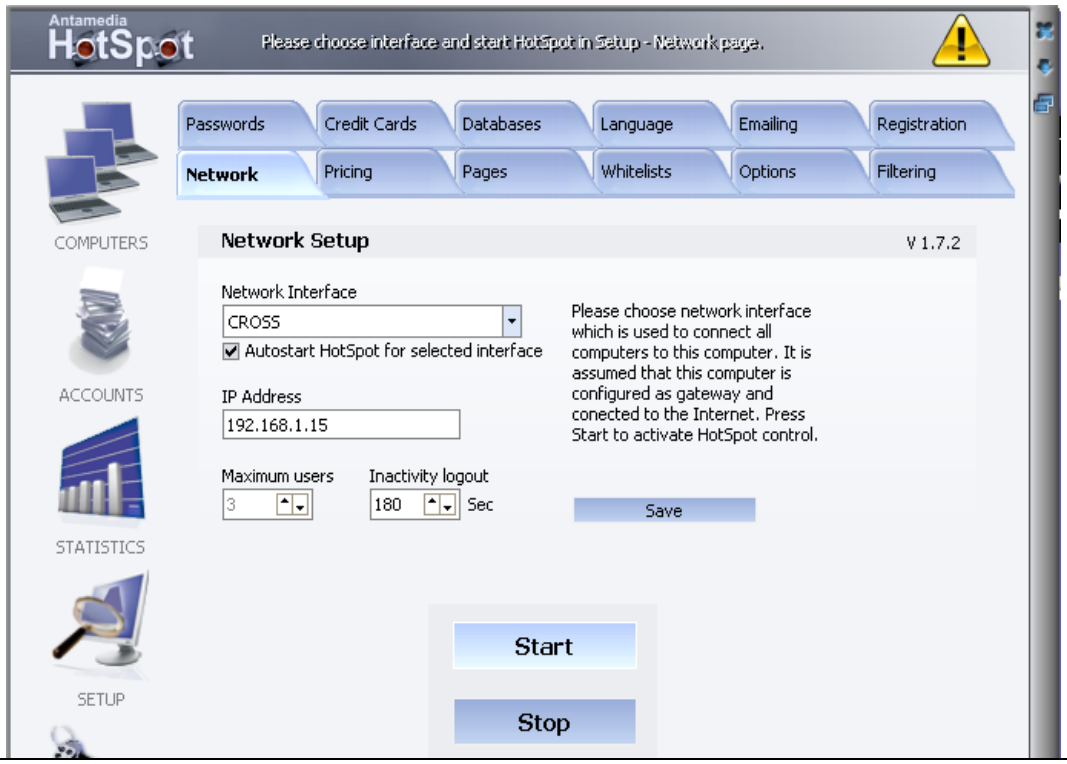

Antamedia HotSpot Installer 1.7.2
License agreement
Please read the following license agreement carefully.
This is End-User License Agreement ("EULA") and is a legal agreement between you (either an individual or a single entity), and ANTAMEDIA as a licensor. By installing, copying or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, do not install, copy or otherwise use Antamedia HotSpot Software.
1. Licensee. For purposes of this License, the term "Licensee" means the person, company or entity that uses the Software under this License. The Licensee must accept and agree to this License before installing or using the Software. License in the form of a product or package label or confirmation e-mail will be sent to the Licensee and will identify the Software licensed to Licensee under this License and the type of license(s) granted to Licensee for each Software product.
2. Software and Documentation. "Software" means the computer programs of the licensed software product(s) in the form and version(s) provided to Licensee, together with the associated media and corresponding Documentation. "Documentation" means the end user manual and other documentation (including print and "online"), if any, provided to Licensee with the Software.
I accept the terms in the license agreement
I do not accept the terms in the license agreement
Next

Chọn Antamedia Hotspot→Next→ Install

Bước 2: Nhấn nút Reboot → Máy tính sẽ khởi động lại→Hotspot→ Login bằng Username là Administrator → Setup →Network



Bước 3: Đánh dấu mục chọn Autostart HotSpot for selected interface→Card mạng kết nối với Wireless Access Point và kiểm tra đúng IP của Card này → Save → Start

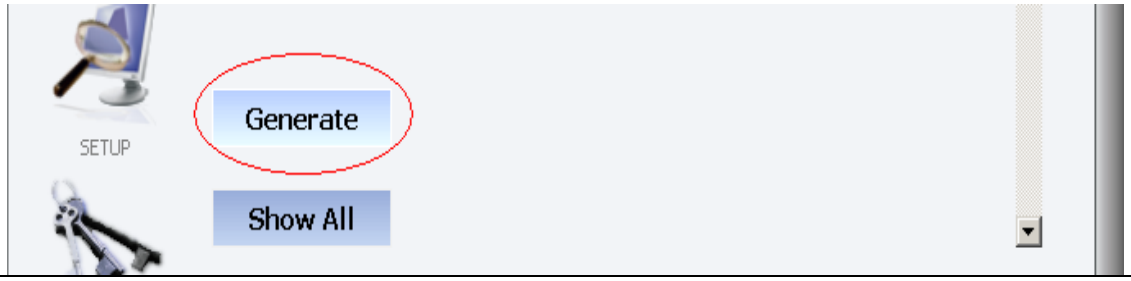


4. 4 Tạo Pricing Plans

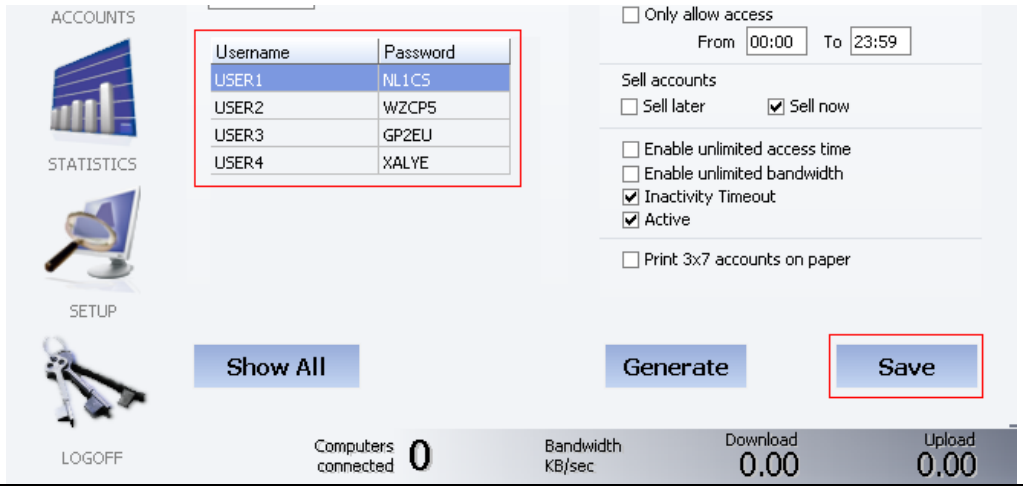
Chọn Setup→ Pricing→Pricing Plan→ qui định các thông số cần thiết theo nhu cầu sau đó nhấn nút Add

4.5 Tạo User Account

Bước 1: Chọn Account →Generate

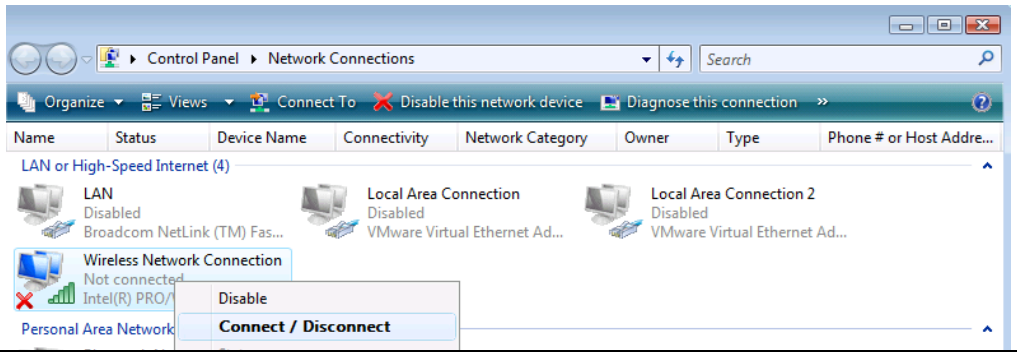


Bước 2: Chọn User đã được tạo ra theo nhu cầu→ Nhấn Save để lưu lại

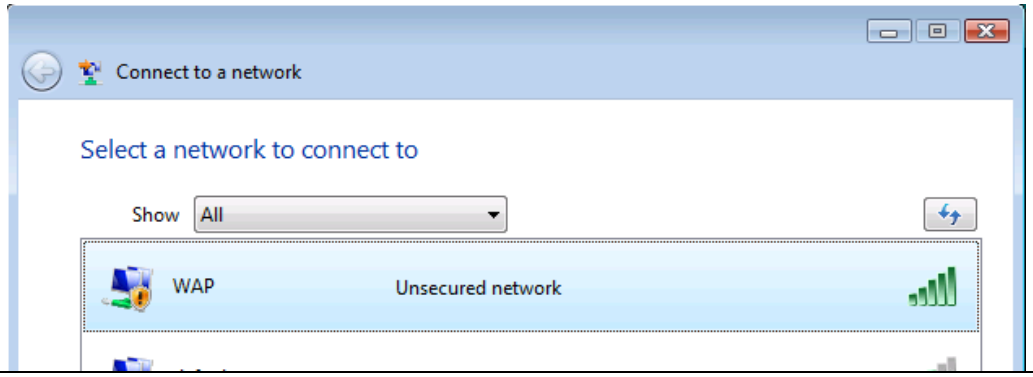


4.6 Kiểm tra trên máy Client

Bước 1: Mở chế độ kết nối Wireless

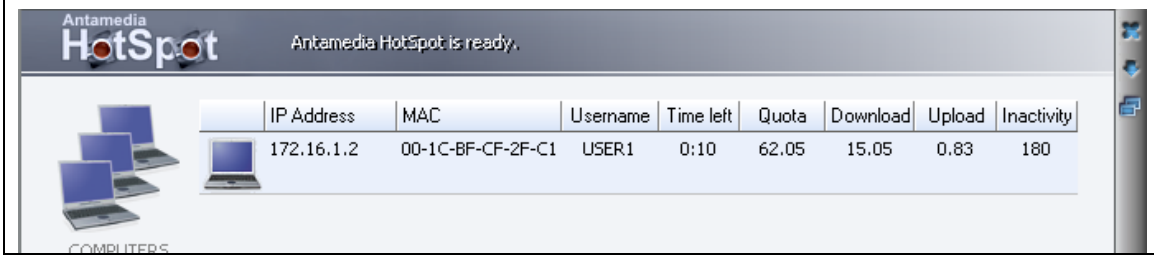


Bước 2: Chọn WAP → nhấn Connect



Bước 3:Truy cập thành công

Lúc này, kết nối từ Client đã được thể hiện trên Wireless Gateway, chọn Computer→ sẽ thấy danh sách các Client đang kết nối với đầy đủ các thông tin cần thiết như IP, MAC, Userv.v



5- TÓM TẮT NỘI DUNG

- Máy tính chỉ ra ngoài internet được khi nó có địa chỉ public vì địa chỉ public là duy nhất, do vậy cần phải có một kỹ thuật để chuyển đổi các IP private trong mạng LAN thành IP public để ra ngoài internet và ngược lại để các máy Internet có thể gửi trả dữ liệu cho các máy trong LAN là NAT(Network Address Translation) ra đời để giải quyết vấn đề này
- NAT hoạt động trên thiết bị kết nối LAN với mạng Internet như ADSL, Router, Firewall..
- NAT xử lý một gói tin xuất phát từ bên trong đi ra bên ngoài

- NAT sẽ xử lý một gói tin xuất phát từ mạng bên ngoài đi vào mạng bên trong
- Lợi ích của NAT:
    - Giảm thiểu hụt địa chỉ của IPv4
    - NAT che giấu IP bên trong LAN.

6- CÂU HỎI VÀ BÀI TẬP

CÂU HỎI

Câu 1: Điều gì sẽ xảy ra khi dùng NAT 2 lớp?

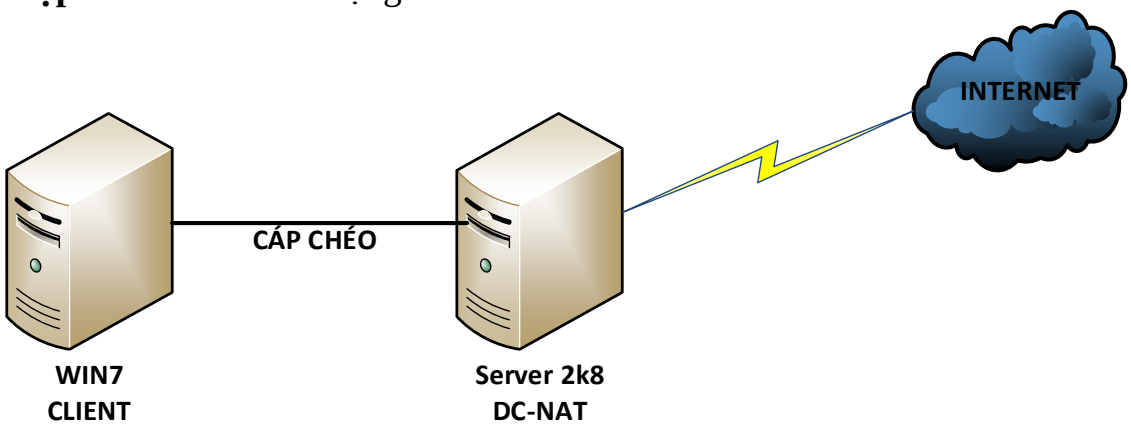
Câu 2: Trình bày cách thức làm việc của NAT**.**

Câu 3: NAT giải quyết những vấn đề nào ?

Câu 4:Trình bày các khái niệm cơ bản về NAT.

BÀI TẬP

Bài tập 1:Cho mô hình mạng



Yêu cầu: Cài đặt và cấu hình NAT trên windows server 2008

Chuẩn bị:

- 1máy PC cài win2k8 nâng cấp lên DC, có 2 card mạng
- 1 máy PC cài win7
- 1 sợi cáp bấm thẳng
- 1 sợi cáp bấm chéo
- Thiết lập địa chỉ IP khác lớp hoặc netID
- Các bước Cấu hình NAT trên windows server 2008:

Hướng dẫn làm bài

1. Cài đặt Routing And Remote Access

2. Cấu hình NAT

B1:Trên giao diện Routing And Remote Access click chuột phải vào tên máy tính HT-SRV-01. Chọn Configure and enable Routing and remote access.

B2:Trên màn hình Welcome chọn Next→Tại màn hình Configuration chọn Custom Configuration→Trên màn hình Custom Configuration chọn NAT→Click chọn Finish.

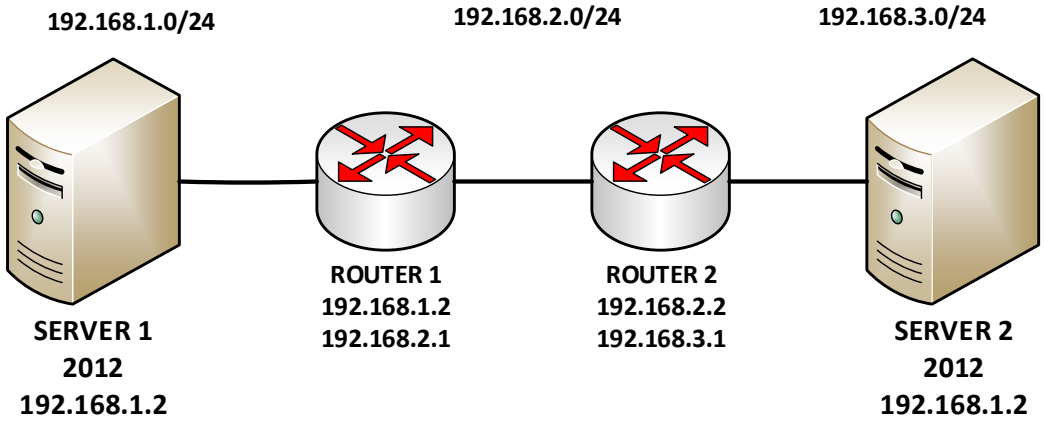
B3:Trên màn hình Routing and Remote Access, mở thanh xổ ra tìm đến NAT. Tại đây chúng ta sẽ gán Interface vào. Click chuột phải vào NAT→chọn new Interface sau đó chọn card Internet→Ở đây card Int là card nằm bên trong, card mà bên ngoài "không nhìn thấy" nên chọn Private sau đó click OK→Tương tự, click chuột phải vào NAT chọn New Interface sau đó chọn card còn lại là Lan→chọn Public interface connect to the internet.

B4:Để kích hoạt NAT trên card Lan, tick chọn Enable NAT on this interface sau đó click OK.

B5:Gán giải IP public chuyển qua tab Address Pool→cho phép dịch vụ có thể đi qua NAT chuyển qua tab Service and Port

B6:Kiểm tra kết nối

Bài tập 2: Cho mô hình mạng



Yêu cầu: Cài đặt và cấu hình NAT trên windows server 2012

Chuẩn bị:

- 2máy PC cài win2k12 nâng cấp, có 2 card mạng
- 2 sợi cáp bấm thẳng
- Thiết lập địa chỉ IP khác netID
- Các bước Cấu hình NAT trên windows server 2012

Hướng dẫn làm bài

1.Cấu hình tính năng Lan routing để định tuyến các phân đoạn mạng trong hệ thống.

B1: Vào Routing and Remote Access trên Server 2012 làm như sau: Run (Ctrl + R) → rrasmgmt.msc

B2: Mặc định tính năng bị disable, ta chọn Configure and Enable Routing and Remote Access→Xuất hiện bàng điều khiển → Next

B3: Các tính năng trong routing and remote access:gồm có Dial-up (quay số), VPN, NAT…→ Custom Configuration

B4: Lan routing → Finish.

2.Cấu Hình Static Routes

B1: Static routes → New static route→ add route.

- **Interface**: gói tin sẽ ra bằng ethernet 2 (tức là card mạng có IP là: 192.168.1.1)
- **Destination:** 192.168.3.2
- **Network mask**: ta đánh: 255.255.255.255.
- **Gateway**: địa chỉ IP của router kết tiếp (tức là con router mà ta hỏi đường)
- **Metric**: độ ưu tiên. Nếu có 2 route cùng đến 1 destination, route nào có metric nhỏ hơn sẽ ưu tiên hơn.

B2: All Tasks → Restart

B3: Ping kiểm tra→ Vào **Static Routes -→ Show IP Routing Table**… để xem bảng định tuyến của Router 1

B4: Ở router 2, muốn đến được Server 1, ta làm tương tự

- **Interface**: gói tin sẽ ra bằng ethernet 2 (tức là card mạng có IP là: 192.168.1.1)
- **Destination:** 192.168.2.0
- **Network mask**: ta đánh: 255.255.255.0.
- **Gateway**: 192.168.1.1
- **Metric**: 256

3.Cấu hình Rip V2.

B1: Trên Router 1:→Chọn General → New Routing Protocol.

B2: RIP Version 2 for Internet Protocol→ chọn RIP -> New Interface..

B3: Chọn card mạng dùng RIP. Ở đây Router 1 giao tiếp với Router 2 để trao đổi bảng định tuyến qua Ethernet 2 bằng giao thức RIP nên ta sẽ cấu hình Ethernet 2 sử dụng RIP

4.Cấu hình tổng quan RIP

B1: Incoming Packet protocol: RIp v1 and 2: nhận update = V1, V2

B2: Activate Authentication: Chứng thực xong mới update, ở đây không cần nên bỏ trống.

B3: Ở router 2 làm tương tự là xong.

BÀI 4 :BẢO VỆ MẠNG BẰNG TƯỜNG LỬA

Mã bài MĐ 26-04

Thời gian :8 giờ

I. MỤC TIÊU: Sau khi học bài học này, sinh viên có khả năng

- Liệt kê được các tình huống tấn công mạng ;
- Trình bày được xây dựng kiến trúc mạng sử dụng tường lửa ;
- Cấu hình tường lửa để bảo vệ mạng.
- Thực hiện các thao tác an toàn với máy tính.

II. NỘI DUNG CHÍNH

1. Các kiểu tấn công

Mục tiêu: Liệt kê được các tình huống tấn công mạng

1.1.Tấn công trực tiếp

Những cuộc tấn công trực tiếp thông thường được sử dụng trong giai đoạn đầu để chiếm được quyền truy nhập hệ thống mạng bên trong.

Điển hình cho tấn công trực tiếp là các hacker sử dụng một phương pháp tấn công cổ đIển là dò tìm cặp tên người sử dụng và mật khẩu thông qua việc sử dụng một số thông tin đã biết về người sử dụng để dò tìm mật khẩu, đây là một phương pháp đơn giản dễ thực hiện.

1.2. Nghe trộm

Thông tin gửi đi trên mạng thường được luân chuyển từ máy tính này qua hàng loạt các máy tính khác mới đến được đích. Điều đó, khiến cho thông tin của ta có thể bị kẻ khác nghe trộm.

1.3. Giả mạo địa chỉ

Giả mạo địa chỉ có thể được thực hiện thông qua sử dụng khả năng dẫn đường trực tiếp. Với cách tấn công này kẻtấn công gửi các gói tin tới mạng khác với một địa chỉ giả mạo, đồng thời chỉ rõ đường dẫn mà các gói tin phải đi.

1.4. Vô hiệu hoá các chức năng của hệ thống

Đây là kiểu tấn công làm tê liệt hệ thống, làm mất khả năng cung cấp dịch vụ (Denial of Service DoS) không cho hệ thống thực hiện được các chức năng mà nó được thiết kế. Kiểu tấn công này rất khó ngăn chặn bởi chính những phương tiện dùng để tổ chức tấn công lại chính là những phương tiện dùng để làm việc và truy cập thông tin trên mạng.

Điều đáng sợ là các kiểu tấn công DoS chỉ cần sử dụng những tài nguyên giới hạn mà vẫn có thể làm ngưng trệ dịch vụ của các site lớn và phức tạp. Do vậy loại hình tấn công này còn được gọi là kiểu tấn công không cân xứng

(asymmetric attack). Chẳng hạn như kẻ tấn công chỉ cần một máy tính PC thông thường với một modem tốc độ chậm vẫn có thể tấn công làm ngưng trệ các máy tính mạnh hay những mạng có cấu hình phức tạp

1.5. Lỗi của người quản trị hệ thống

Không thay đổi các mật khẩu mặc định trên tất cả các thiết bị mạng:

Có rất nhiều công ty giữ nguyên mật khẩu mặc định cho các thiết bị mạng trong công ty là "password" hay "admin". Để tránh được vấn đề này, bạn cần quét lại tất cả các thiết bị mạng có địa chỉ IP không chỉ riêng với hệ thống quan trọng hay có kết nối với Internet. Sau đó bạn cần đổi tất cả các mật khẩu mặc định trên các thiết bị đó.

Chia sẻ mật khẩu trên các thiết bị mạng

Bộ phận kỹ thuật thường có thói quen dùng chung mật khẩu cho tất cả các Sever trên mạng và thậm chí có một vài người biết các mật khẩu đó. Tuy đó có thể là những mật khẩu mạnh nhưng khi nó được dùng chung thì nó có thể bị phá hoại bất kỳ lúc nào. Có thể nhờ lỗ hổng này mà tin tặc có thể tìm được mật khẩu và gây ra những tổn thất khôn lường cho công ty.

Cho phép truy cập từ xa và các phần mềm quản trị không an toàn

Một trong những cách phổ biến nhất để tin tặc có thể xâm nhập vào trong mạng là việc cho phép truy cập từ xa và sử dụng các gói phần mềm quản lý như PCAnywhere, VNC, SSH. Cách đơn giản nhất đề tìm ra vấn đề này là quét toàn bộ không gian địa chỉ IP để tìm ra những ứng dụng PCAnywhere, VNC hay SSH, đặt các biện pháp an ninh hoặc thêm chế độ xác thực mật khẩu cho chúng. Một lựa chọn nữa là quét toàn bộ luồng dữ liệu của các thiết bị định tuyến.

Không kiểm tra các ứng dụng thông thường

Các nhà quản trị mạng cho biết, vấn đề lớn nhất của họ là các ứng dụng trên Web. Do đó họ dồn tất cả nỗ lực của mình để kiểm tra những hệ thống quan trọng luôn phải "giáp mặt" với Internet. Nhưng vấn đề là hầu hết các cuộc tấn công lại nhằm vào những sơ hở trên hệ thống không quan trọng bên trong mạng lưới.

Không bảo vệ được máy chủ trước những phần mềm độc hại

Hầu hết các phần mềm phá hoại được tin tặc cài đặt từ xa và sử dụng để đánh cắp dữ liệu. Có một cách để các nhà quản trị mạng có thể tìm ra các phần mềm độc hại trên máy chủ là chạy các ứng dụng cảnh báo đột nhập trên tất cả các máy chủ. Một cách đơn giản nữa để ngăn chặn sự tấn công này là khoá máy chủ để không một ứng dụng mới nào có thể cài đặt và chạy trên máy chủ khi chưa được phép.

Không cấu hình định tuyến để chặn các truy cập không mong muốn ra mạng ngoài

Một trong những cách hoạt động phổ biến của các phần mềm độc hại liên quan đến khả năng thực hiện những mệnh lệnh đã được cài sẵn trên các máy chủ. Một cách để ngăn chặn tin tặc lợi dụng sơ hở này là phân chia mạng sử dụng danh sách kiểm soát truy cập. Bằng cách này có thể ngăn chặn máy chủ gửi và phát tán mã độc. Một lựa chọn khác là có thể khoá tất cả các truy cập không cần thiêt ra mạng ngoài..

1.6. Tấn công vào yếu tố con người

Đây là một hình thức tấn công nguy hiểm nhất nó có thể dẫn tới những tổn thất hết sức khó lường. Kẻ tấn công có thể liên lạc với người quản trị hệ thống thay đổi một số thông tin nhằm tạo điều kiện cho các phương thức tấn công khác.

Ngoài ra, điểm mấu chốt của vấn đềan toàn, an ninh trên mạng chính là người sửdụng. Họ là điểm yếu nhất trong toàn bộ hệ thống do kỹ năng, trình độ sử dụng máy tính, bảo mật dữ liệu không cao. Chính họ đã tạo điều kiện cho những kẻ phá hoại xâm nhập được vào hệ thống thông qua nhiều hình thức khác nhau như qua email hoặc sử dụng những chương trình không rõ nguồn gốc, thiếu độ an toàn.

Với kiểu tấn công như vậy sẽ không có bất cứ một thiết bị nào có thể ngăn chặn một cách hữu hiệu chỉ có phương pháp duy nhất là hướng dẫn người sử dụng mạng về những yêu cầu bảo mật để nâng cao cảnh giác. Nói chung yếu tố con người là một đIểm yếu trong bất kỳ một hệ thống bảo vệ nào và chỉ có sự hướng dẫn của người quản trị mạng cùng với tinh thần hợp tác từ phía người sử dụng mới có thể nâng cao độan toàn của hệ thống bảo vệ.

2. Các mức bảo vệ an toàn

Mục tiêu : Trình bày được xây dựng kiến trúc mạng sử dụng tường lửa

Xây dựng giải pháp:

Firewall

Nhiệm vụ của firewall là ngăn chặn các tấn công trực tiếp vào các thông tin quan trọng của hệ thống, kiểm soát các thông tin ra vào hệ thống. Việc lựa chọn firewall thích hợp cho một hệ thống không phải là dễ dàng. Các firewall đều phụ thuộc trên một môi trường, cấu hình mạng, ứng dụng cụ thể. Khi xem xét lựa chọn một firewall, cần tập trung tìm hiểu tập các chức năng của firewall, tính năng lọc địa chỉ, gói tin, ...

Mạng riêng ảo (VPN)

Việc sử dụng VPN để cung cấp cho các nhân viên hay các cộng sự truy cập tới các tài nguyên của công ty từ nhà hay nơi làm việc khác với mức bảo mật cao, hiệu quả nhất trong quá trình truyền thông, và làm tăng hiệu quả sản xuất của nhân viên. Tuy nhiên, không có điều gì không đi kèm sự rủi ro. Bất kỳ tại thời điểm nào khi một VPN được thiết lập, mà phải mở rộng phạm vi kiểm soát bảo mật của công ty tới toàn bộ các nút được kết nối với VPN.

Kiểm tra máy chủ

Sự kiểm tra đều đặn mức bảo mật được cung cấp bởi các máy chủ phụ thuộc chủ yếu vào sự quản lý. Mọi máy chủ ở trong một công ty nên được kiểm tra từ Internet để phát hiện lỗ hổng bảo mật. Thêm nữa, việc kiểm tra từ bên trong và quá trình thẩm định máy chủ về căn bản là cần thiết để giảm thiểu tính rủi ro của hệ thống, như khi firewall bị lỗi hay một máy chủ, hệ thống nào đó bị trục trặc.

Kiểm soát ứng dụng

Việc điều khiển cấu hình bảo mật các ứng dụng có thể làm tăng mức bảo mật. Hầu hết các ứng dụng được cấu hình tại mức tối thiểu của tính năng bảo mật, nhưng qua các công cụ cấu hình, mức bảo mật của hệ thống có thể được tăng lên. Lượng thông tin kiểm soát được cung cấp bởi ứng dụng cũng có thể được cấu hình. Nơi mà các ứng dụng cung cấp thông tin về quy mô bảo mật, thời gian kiểm soát và sự phân tích thông tin này sẽ là chìa khoá để kiểm tra các vấn đề bảo mật thông tin.

Các hệ điều hành

Khi lựa chọn một hệ điều hành, hãy tìm hiểu không chỉ các tiêu chuẩn thông thường như (quản trị, hiệu năng, tính chứng thực), mà còn phải xem xét khả năng áp dụng được của hệ điều hành với hệ thống hiện tại. Một hệ điều hành có thể cung cấp cơ chế bảo mật tốt hơn khi nó tương thích với các ứng dụng chạy bên trong nó như DNS hay WebServer, trong khi các hệ điều hành khác có thể có nhiều chức năng tốt hơn như một hệ thống application, database hay email server.

3. Internet Firewall

Mục tiêu :Trình bày các thành phần và nguyên tắc hoạt động của tường lửa

3.1 Định nghĩa

Một tường lửa Internet có thể giúp ngăn chặn người ngoài trên Internet không xâm nhập được vào máy tính của bạn. Tường lửa có hai loại, phần mềm hoặc phần cứng, có tác dụng như một biên giới bảo vệ và lọc những kẻ xâm nhập không mong muốn trên Internet.

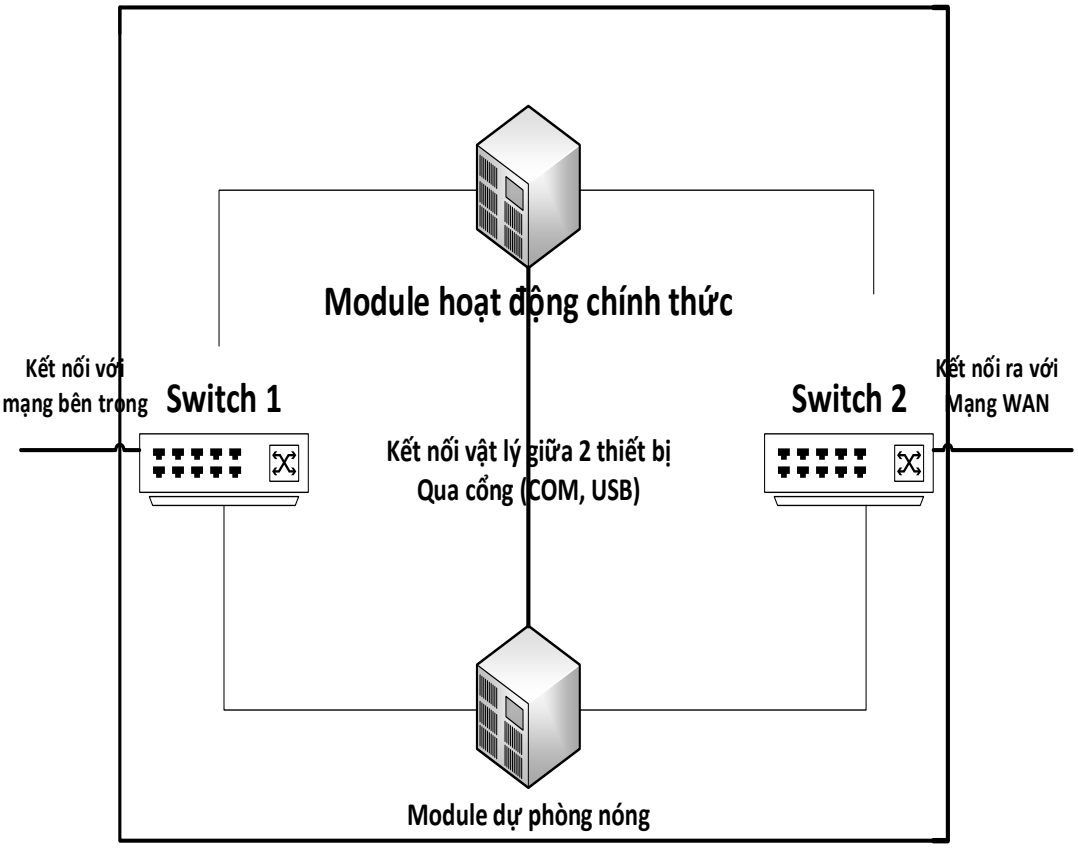
3.2 Chức năng

1. Cho phép hoặc cấm các dịch vụ truy cập ra ngoài.
2. Cho phép hoặc cấm các dịch vụ từ ngoài truy cập vào trong.
3. Theo dõi luồng dữ liệu giữ môi trường intranet và internet .
4. Kiểm soát địa chỉ truy cập, cấm hoăc cho phép địa chỉ được truy nhập.
5. Kiểm soát người dùng và việc truy cập của người dùng.
6. Kiểm soát nội dung thông tin , gói tin lưu chuyển trên hệ thống mạng.

7. Lọc các gói tin dựa vào địa chỉ nguồn, địa chỉ đích và số cổng (port), giao thức
8. Có thể sử dụng để ghi lại tất cả các sự cố gắng truy nhập vào mạng và báo cáo cho người quản trị

3.3 Cấu trúc

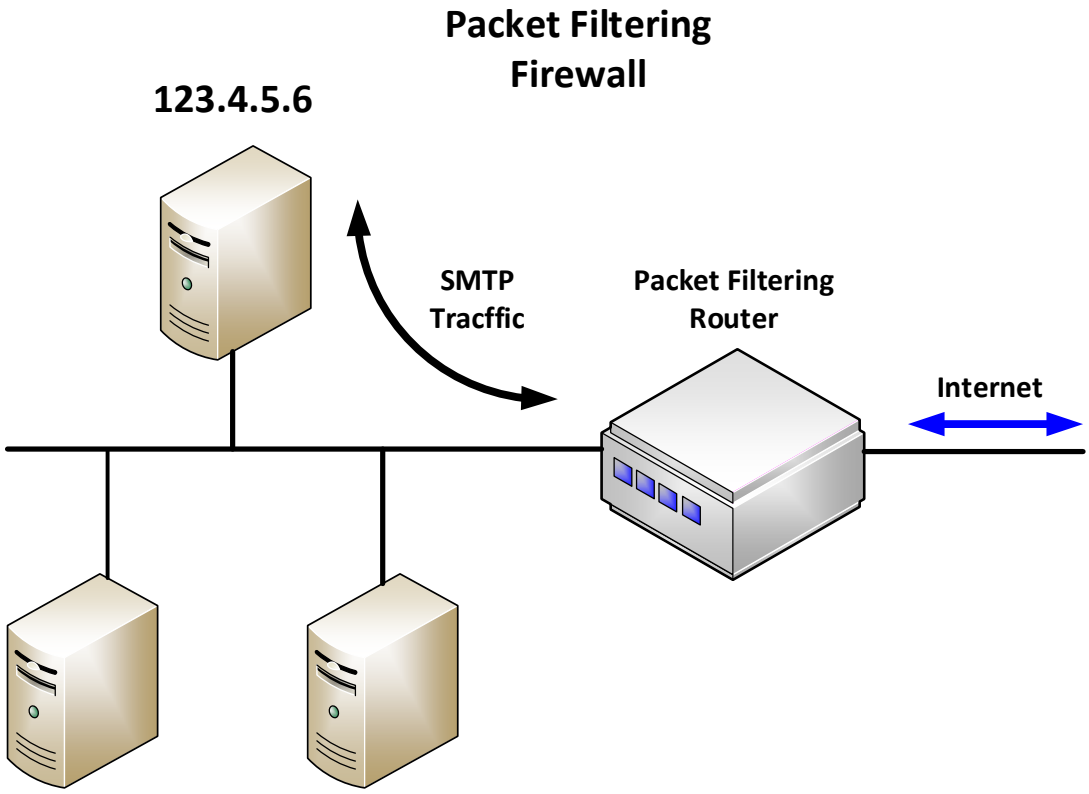
Đây là một loại Firewall được thiết kế để tăng cường chức năng kiểm soát các loại dịch vụ, giao thức được cho phép truy cập vào hệ thống mạng. Cơ chế hoạt động của nó dựa trên cách thức gọi là Proxy service. Proxy service là các bộ code đặc biệt cài đặt trên gateway cho từng ứng dụng. Nếu người quản trị mạng không cài đặt proxy code cho một ứng dụng nào đó, dịch vụ tương ứng sẽ không được cung cấp và do đó không thể chuyển thông tin qua firewall. Ngoài ra, proxy code có thể được định cấu hình để hỗ trợ chỉ một số đặc điểm trong ứng dụng mà người quản trị mạng cho là chấp nhận đợc trong khi từ chối những đặc điểm khác. Mỗi proxy đều độc lập với các proxies khác trên bastion host. Điều này cho phép dễ dàng quá trình cài đặt một proxy mới, hay tháo gỡ môt proxy đang có vấn đề



Hình 4-1:sơ đồ hoạt động tường lửa

3.4. Các thành phần của Firewall và cơ chế hoạt động

3.4.1. Bộ lọc Paket (Paket filtering router)



Hình 4-2:sơ đồ lọc gói của tường lửa

Bộ lọc packet cho phép hay từ chối mỗi packet mà nó nhận được. Nó kiểm tra toàn bộ đoạn dữ liệu để quyết định xem đoạn dữ liệu đó có thoả mãn một trong số các luật lệ của lọc packet hay không. Các luật lệ lọc packet này là dựa trên các thông tin ở đầu mỗi packet (packet header), dùng để cho phép truyền các packet đó ở trên mạng. Đó là:

+ Địa chỉ IP nơi xuất phát (IP Source address)
+ Địa chỉ IP nơi nhận (IP Destination address)
+ Những thủ tục truyền tin (TCP, UDP, ICMP, IP tunnel)
+ Cổng TCP/UDP nơi xuất phát (TCP/UDP source port)
+ Cổng TCP/UDP nơi nhận (TCP/UDP destination port)
+ Dạng thông báo ICMP (ICMP message type)
+ Giao diện packet đến (incomming interface of packet)
+ Giao diện packet đi (outcomming interface of packet)

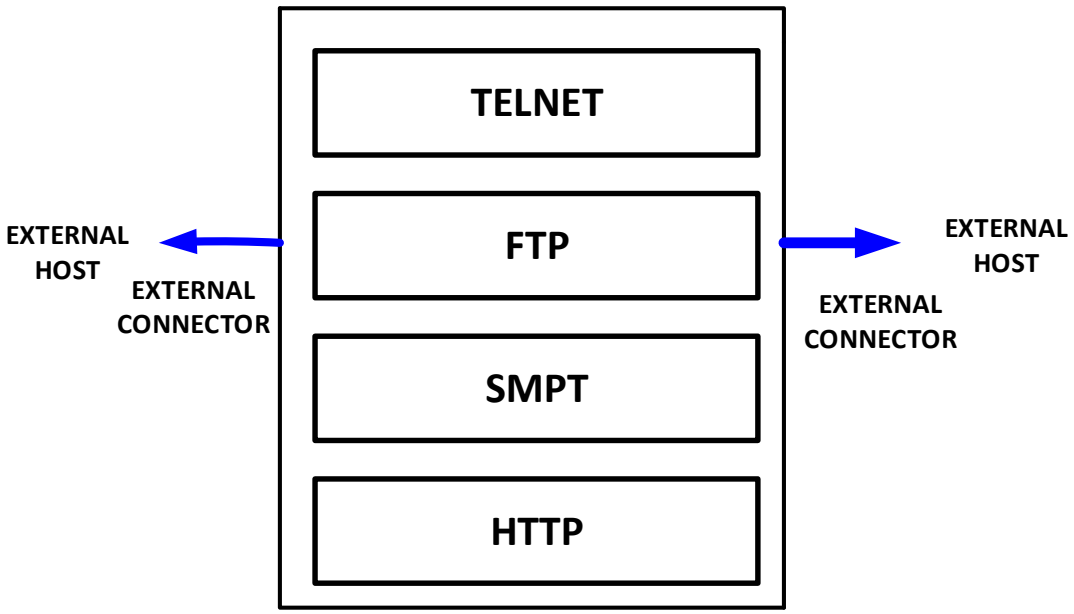
Ưu điểm

+ Đa số các hệ thống firewall đều sử dụng bộ lọc packet. Một trong những ưu điểm của phương pháp dùng bộ lọc packet là chi phí thấp vì cơ chế lọc packet đã được bao gồm trong mỗi phần mềm router.
+ Ngoài ra, bộ lọc packet là trong suốt đối với người sử dụng và các ứng dụng, vì vậy nó không yêu cầu sự huấn luyện đặc biệt nào cả.

Hạn chế

+ Việc định nghĩa các chế độlọc package là một việc khá phức tạp; đòi hỏi người quản trị mạng cần có hiểu biết chi tiết về các dịch vụ Internet, các dạng packet header, và các giá trị cụ thể có thể nhận trên mỗi trường. Khi đòi hỏi về sự lọc càng lớn, các luật lệ về lọc càng trở nên dài và phức tạp, rất khó để quản lý và điều khiển.
+ Do làm việc dựa trên header của các packet, rõ ràng là bộ lọc packet không kiểm soát được nôi dung thông tin của packet. Các packet chuyển qua vẫn có thể mang theo những hành động với ý đồ ăn cắp thông tin hay phá hoại của kẻ xấu.

3.4.2. Cổng ứng dụng (Application- Level Getway)



Hình 4-3:sơ đồ cổng ứng dụng

Ưu điểm

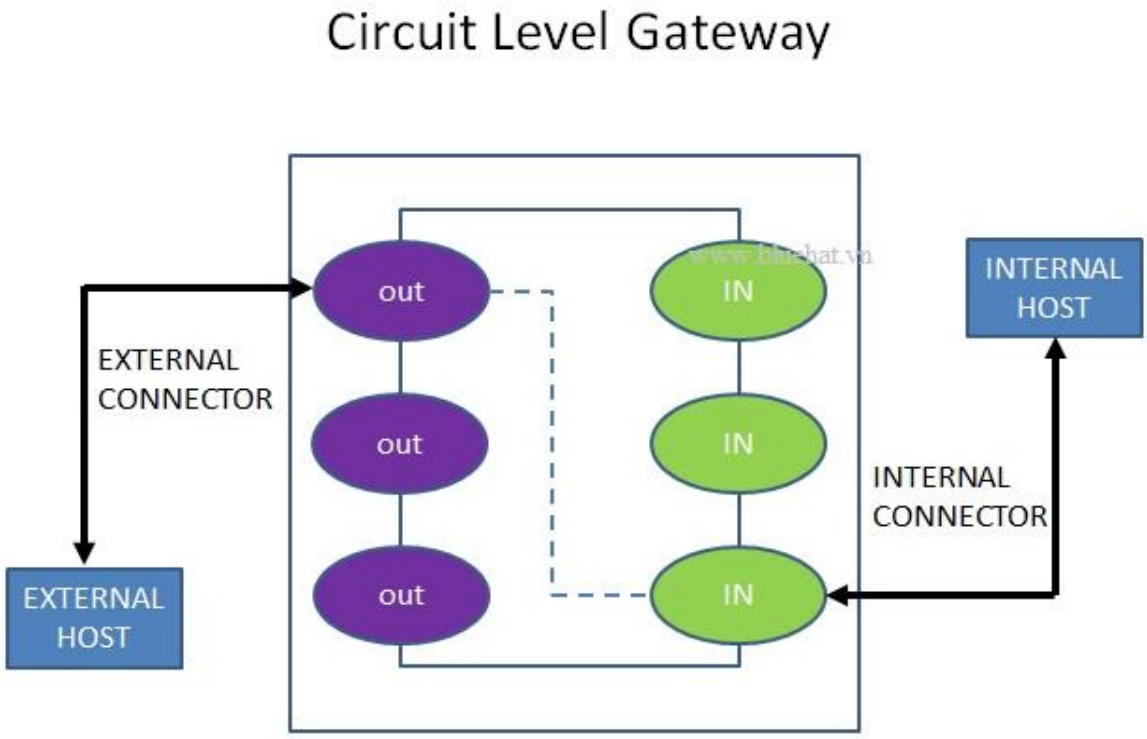
+ Cho phép người quản trị mạng hoàn toàn điều khiển được từng dịch vụ trên mạng, bởi vì ứng dụng proxy hạn chế bộ lệnh và quyết định những máy chủ nào có thể truy nhập được bởi các dịch vụ.

+ Cho phép người quản trị mạng hoàn toàn điều khiển được những dịch vụ nào cho phép, bởi vì sự vắng mặt của các proxy cho các dịch vụ tương ứng có nghĩa là các dịch vụ ấy bị khoá.
+ Cổng ứng dụng cho phép kiểm tra độ xác thực rất tốt, và nó có nhật ký ghi chép lại thông tin về truy nhập hệ thống.
+ Luật lệ lọc filltering cho cổng ứng dụng là dễ dàng cấu hình và kiểm tra hơn so với bộ lọc packet.

Hạn chế

Yêu cầu các users thay đổi thao tác, hoặc thay đổi phần mềm đã cài đặt trên máy client cho truy nhập vào các dịch vụ proxy. Chẳng hạn, Telnet truy nhập qua cổng ứng dụng đòi hỏi hai bước để nối với máy chủ chứ không phải là một bước thôi. Tuy nhiên, cũng đã có một số phần mềm client cho

3.4.3. Cổng vòng (Circult-level Getway)



Hình 4-4:sơ đồ cổng vòng

Cổng vòng là một chức năng đặc biệt có thể thực hiện được bởi một cổng ứng dụng. Cổng vòng đơn giản chỉ chuyển tiếp (relay) các kết nối TCP mà không thực hiện bất kỳ một hành động xử lý hay lọc packet nào.

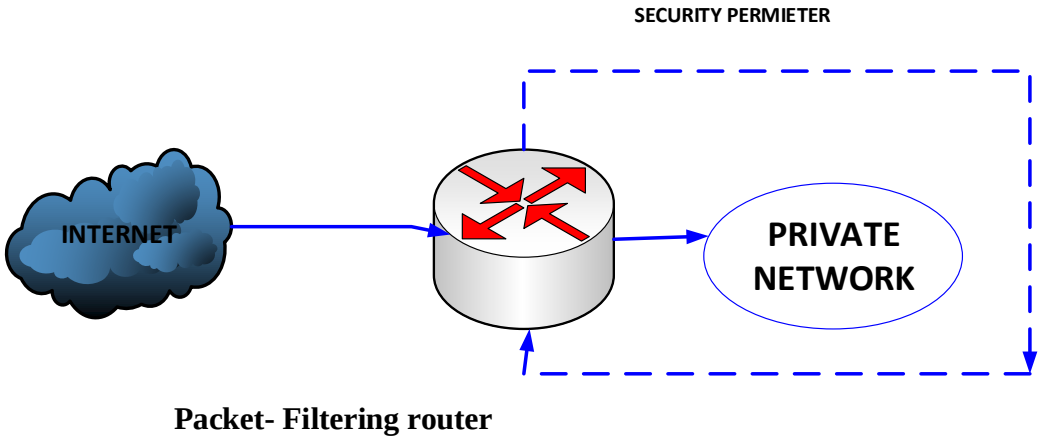
3.5. Những hạn chế của Firewall

+ Firewall không thể ngăn chặn một cuộc tấn công nếu cuộc tấn công này không "đi qua" nó. Một cách cụ thể, firewall không thể chống lại một cuộc tấn công từ một đường dial-up, hoặc sự dò rỉ thông tin do dữ liệu bị sao chép bất hợp pháp.

+ Firewall cũng không thể chống lại các cuộc tấn công bằng dữ liệu (data-drivent attack). Khi có một số chương trình được chuyển theo thư điện tử, vượt qua firewall vào trong mạng được bảo vệ và bắt đầu hoạt động ở đây.

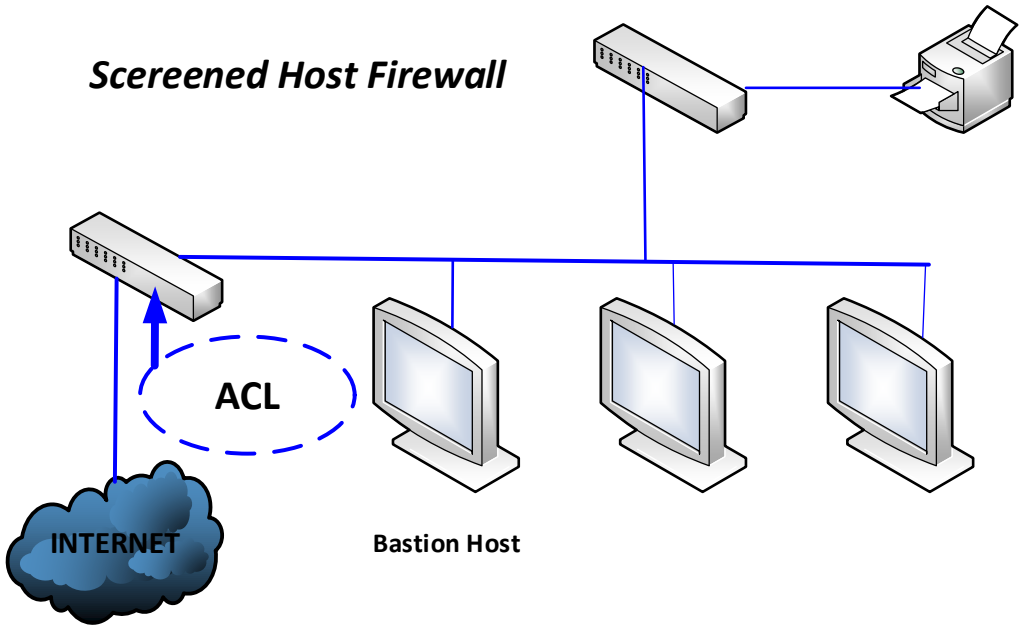
3.6. Các ví dụ về Firewall

3.6.1. Packet- Filtering router (Bộ trung chuyển có lọc gói)



Hình 4-5:sơ đồ bộ trung chuyển có gói lọc

3.6.2. Screened host firewall

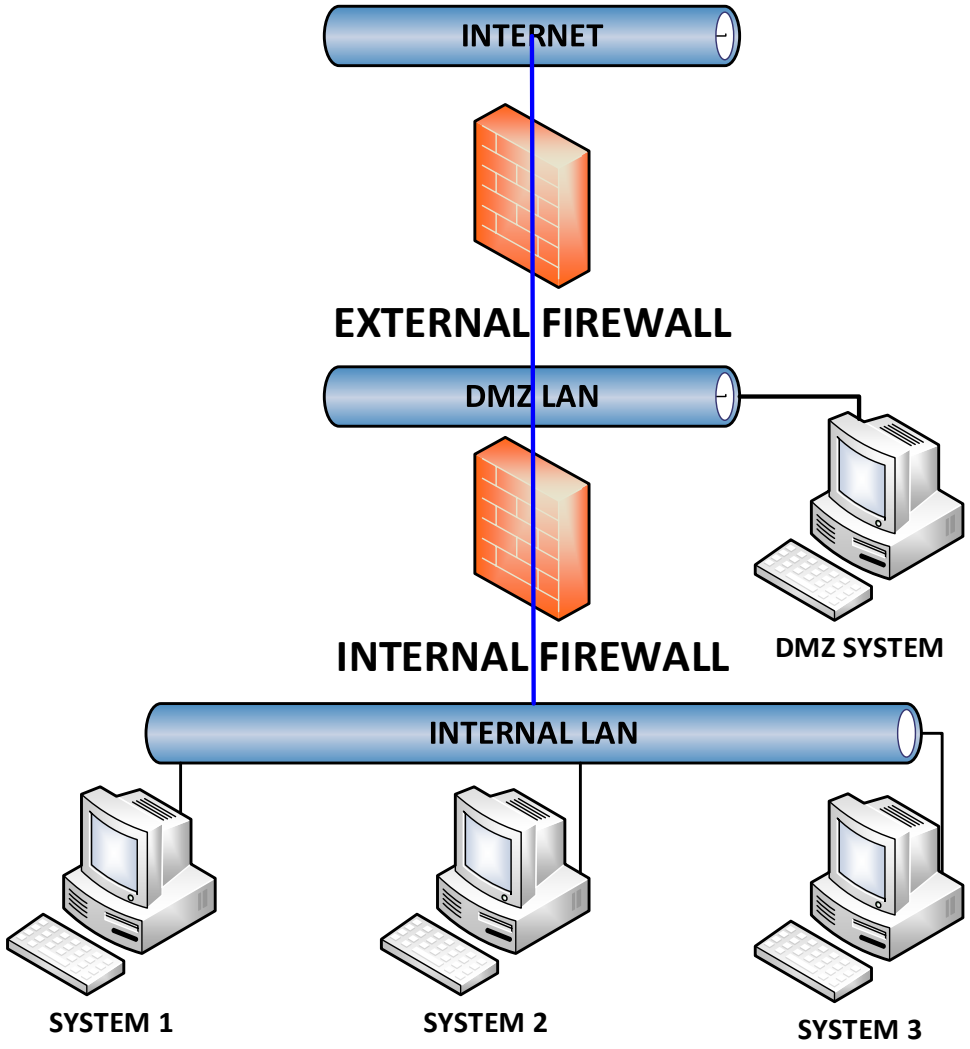


Hình 4-6:sơ đồ hoạt động gói lọc

+ Gồm một Packet Filtering và một bastion host
+ Thực hiện bảo vệ mạng ở tầng mạng và tầng ứng dụng
+ Cấu hình và hoạt động Packet Filtering :

+ Đối với luồng thông tin từ Internet, chỉ các gói tin IP với địa chỉ đích là bastion host mới được phép đi vào trong
+ Đối với luồng thông tin từ bên trong, chỉ các gói tin IP xuất phát từ bastion host mới được phép đi ra ngoài
+ Packet Filtering cho phép bastion host mở kết nối (hợp lệ) ra bên ngoài.
+ Packet Filtering có thể cho phép các internal hosts mở kết nối đến các host trên internet đối với 1 số dịch vụ được phép hoặc cấm tất cả kết nối từ các internal hosts.

3.6.3. Demilitarized Zone (DMZ – khu vực phi quân sự)



Hình 4-7:sơ đồ đặt vùng của tường lửa

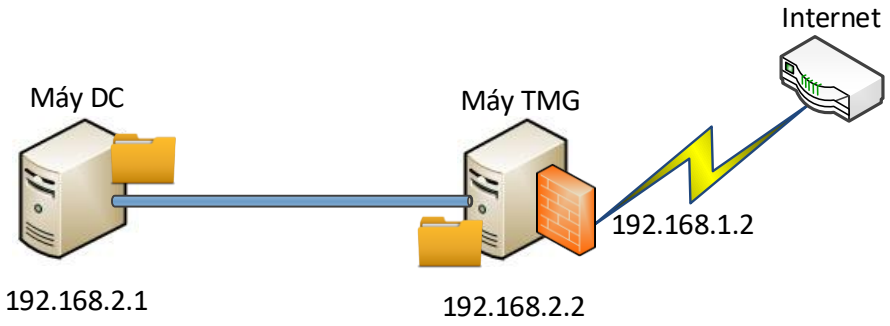
DMZ là một mạng tách biệt với mạng internal vì DMZ sử dụng đường mạng (hoặc có subnet) khác với mạng internal. Và các server như Web, Mail, FTP, VoIP… là các dịch vụ tổ chức mong muốn người dùng có thể truy cập và sử dụng thông qua các mạng ngoài như Internet được đặt trong vùng DMZ. Còn các server phục vụ cho các mục đích nội bộ như DNS, DHCP, File/Print… vẫn được đặt trong vùng internal.

Giữa DMZ và mạng external ta có thể đặt một firewall để cho phép các kết nối từ external chỉ đến được DMZ mà thôi. Còn giữa mạng internal và DMZ ta có thể đặt thêm một firewall khác để kiểm soát các lưu lượng từ DMZ đi vào internal.

Như vậy, cũng giống với vùng DMZ trong quân sự, DMZ ở đây đã tạo ra sự phân tách giữa hai bên đối nghịch nhau: mạng internal và mạng external. Và có thể nói rằng DMZ đã bổ sung thêm một lớp bảo vệ cách ly cho mạng internal khi mà hacker từ mạng ngoài chỉ có thể tiếp cận tới các máy nằm trong DMZ mà thôi.

4. Bài tập thực hành

Bài tập 1: cho mô hình mạng như sau



Yêu cầu: Cài đặt, cấu hình tạo rule cho Admin đi ra ngoài Internet

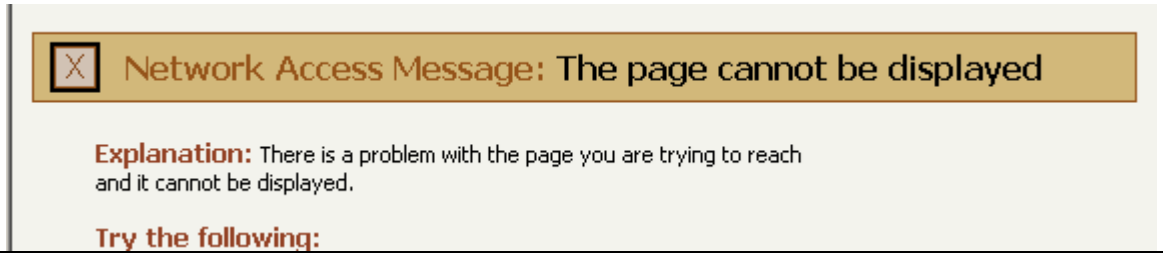
Chuẩn bị:

- 1 máy PC cài đặt win2k8→DC
- 1 máy PC cài đặt win2k8→ cài đặt TMG 2010
- 1 sợi cáp thẳng
- 1 sợi cáp chéo
- Router internet

Thực hiện:

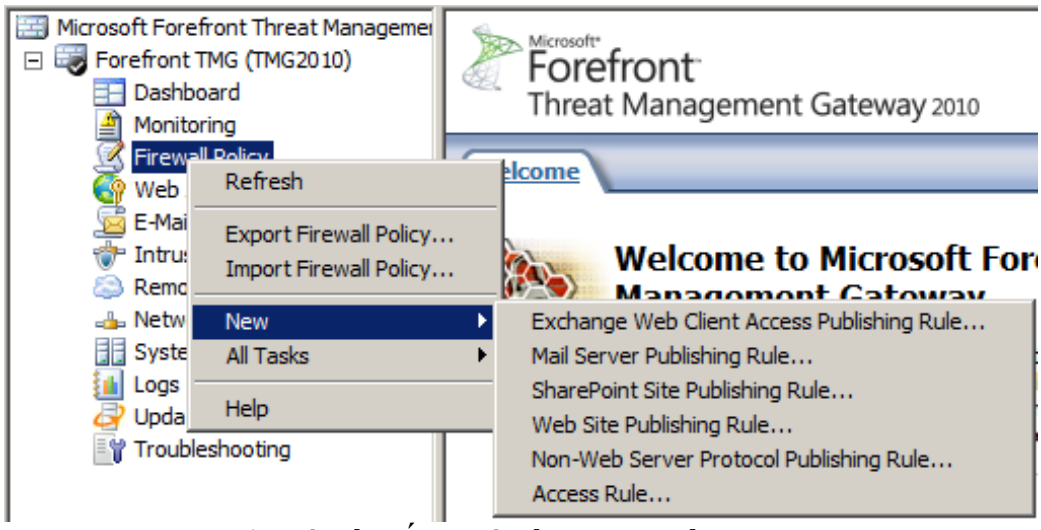
1.Cài đặt, cấu hình tạo rule cho phép ping địa chỉ IP và chia sẻ dữ liệu

Bước 1: Kiểm tra kết nối internet trên máy TMG và máy DC


Network Access Message: The page cannot be displayed
Explanation: There is a problem with the page you are trying to reach and it cannot be displayed.
Try the following:

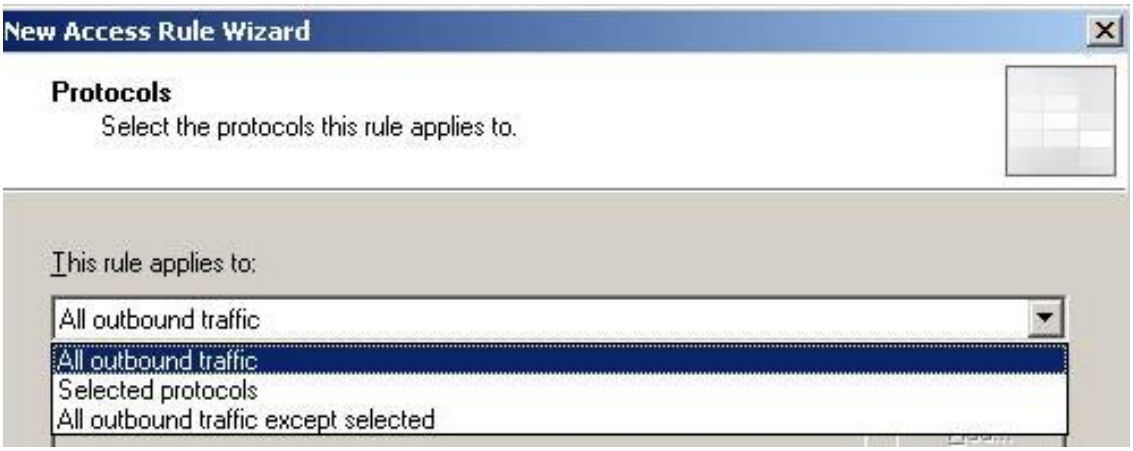
Bước 2: Cài đặt Rule→Click phải chuột vào Firewall Policy→New

→Access Rule

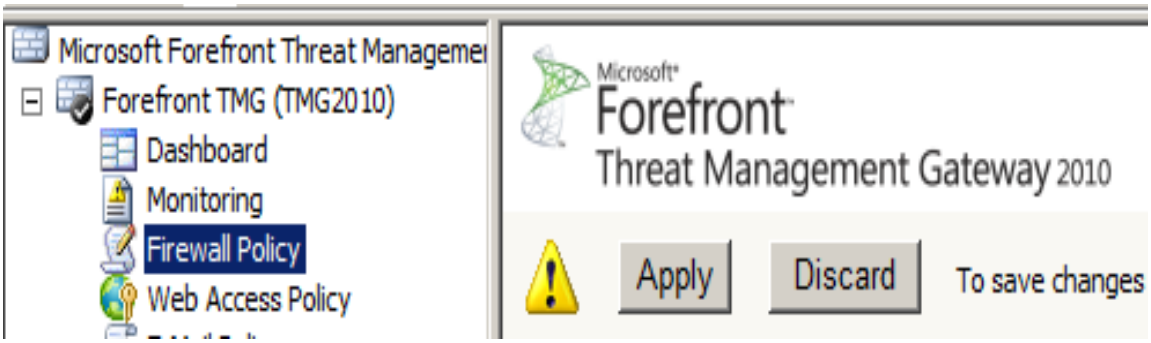


đặt tên→ cấp phép→All user→Finish

Bước 3: Cấu hình Rule→Hộp thoại New Access Rule Winzard→All out bound traffic →Next → Internal→Add→Close→Next→



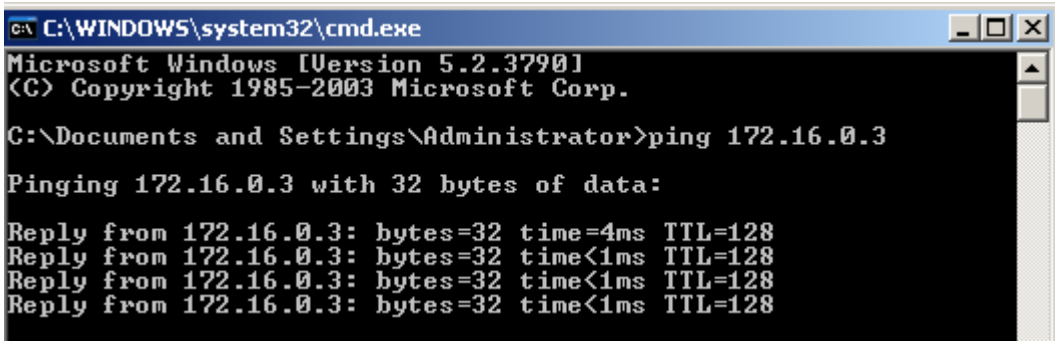
Bước 4: Hoàn tất tạo Rule→ User Sets: Mặc định cho phép tất cả User → Next→Finish



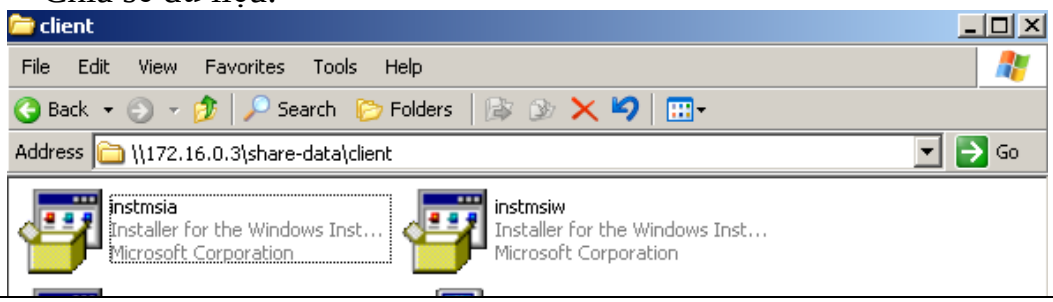
Chọn OK. Để cập nhật

Bước 5: Kiểm tra thông mạng

+ Trên máy DC ping địa chỉ IP máy TMG→thông mạng

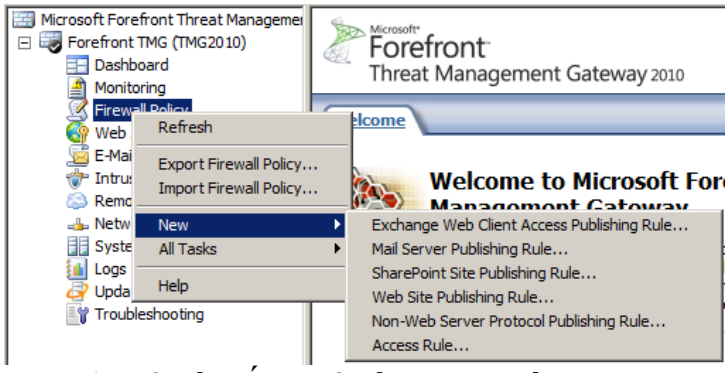

C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
C:\Documents and Settings\Administrator>ping 172.16.0.3
Pinging 172.16.0.3 with 32 bytes of data:
Reply from 172.16.0.3: bytes=32 time=4ms TTL=128
Reply from 172.16.0.3: bytes=32 time<1ms TTL=128
Reply from 172.16.0.3: bytes=32 time<1ms TTL=128
Reply from 172.16.0.3: bytes=32 time<1ms TTL=128

+ Chia sẻ dữ liệu.



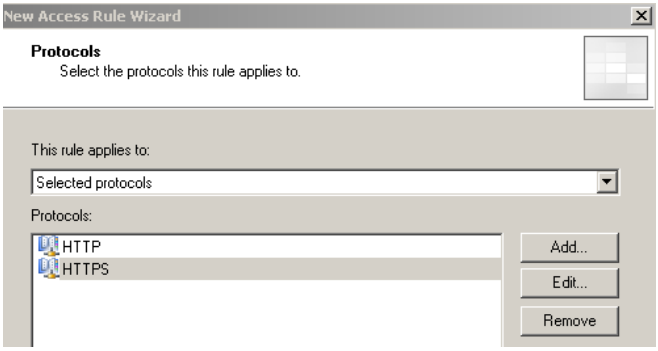
2. Cài đặt, cấu hình tạo rule cho máy domain ra ngoài internet

Bước 1: Cài đặt Rule→Click phải chuột vào Firewall Policy→New →Access Rule



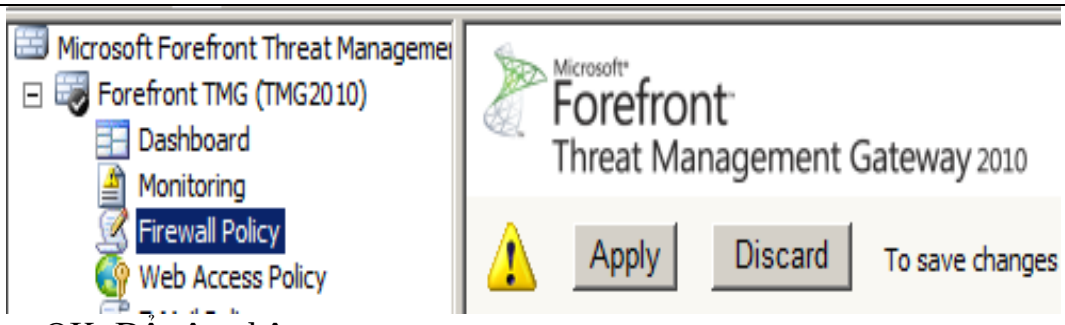
đặt tên→ cấp phép→All user→Finish

Bước 2: Cấu hình Rule→Hộp thoại New Access Rule→ Selected protocols →HTTP, HTTPS→Add →Close→next



Chọn Internal, Local Host→ Add → Close→ Next

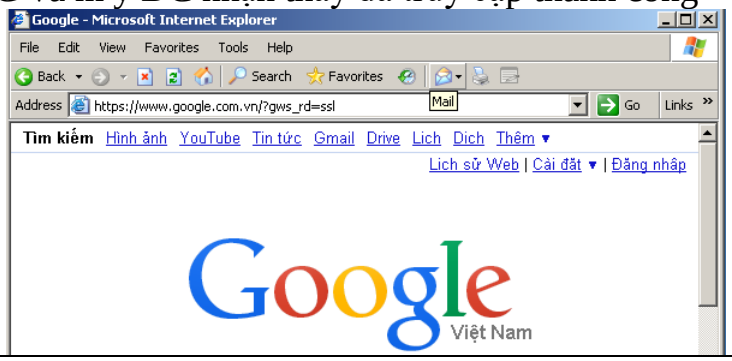
Bước 3: Hoàn tất tạo Rule→ User Sets: Mặc định cho phép tất cả User → Next→Finish



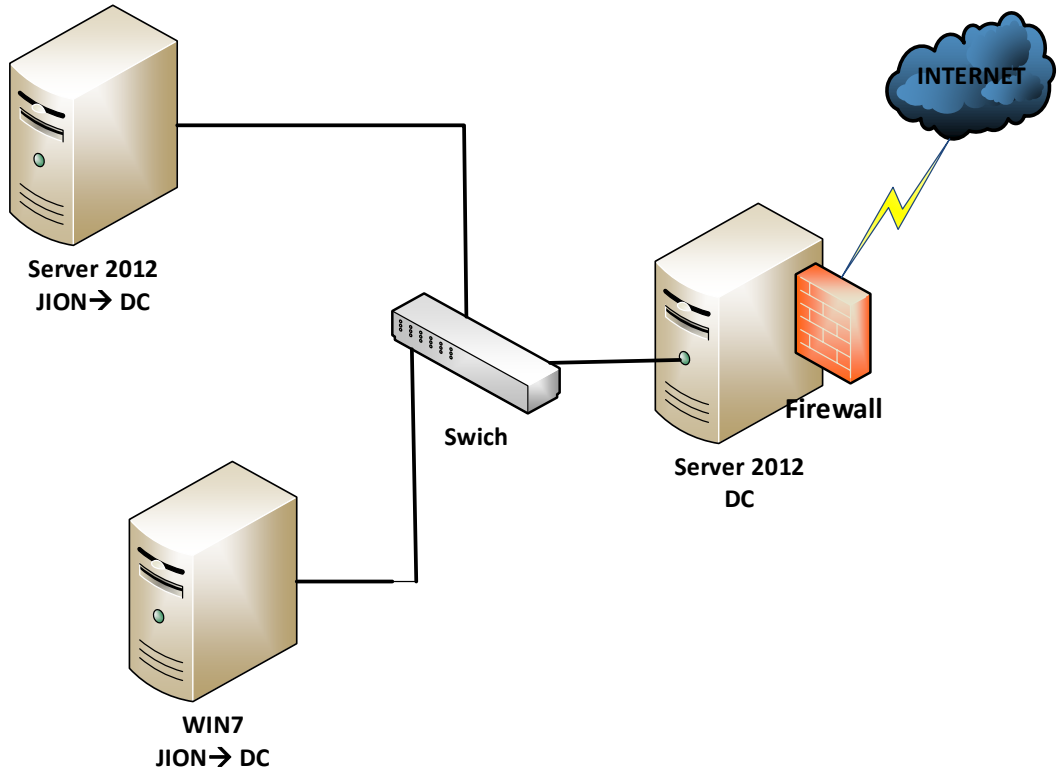
Chọn OK. Để cập nhật

Bước 4: Kết nối intenet

Trên máy TMG và m y DC nhận thấy đã truy cập thành công


Google - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://www.google.com.vn/?gws_rd=ssl
Tìm kiếm Hình ảnh YouTube Tin tức Gmail Drive Lịch Dịch Thêm
Lịch sử Web | Cài đặt | Đăng nhập
Google
Việt Nam

Bài tập 2:Cho mô hình mạng



Yêu cầu:

- Tạo các Isolation rule để chỉ định máy tính nào bị cô lập với các máy tính khác dựa trên các thành viên trong cơ sở hạ tầng Active Directory
- Tạo các Connection security rules để cách ly các máy server

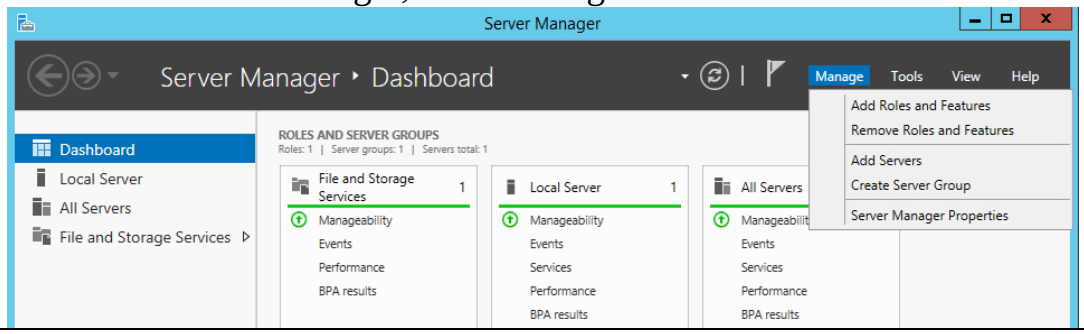
Chuẩn bị:

- Một máy Windows Server 2012, đã nâng cấp thành Domain Controller (DC) với tên miền là tên sinh viên.
- Một máy Windows Server 2012, đã join domain trên.
- Một máy Windows 7, đã join domain trên.
- 1 switch
- 1 router internet
- sợi dây cáp bấm thẳng
- Các thông số IP

	Windows 7 (w7-c1)	**Windows Server 2012 (2k12-sv1)**	**Windows Server 2012 (2k12-sv2)**
IP	192.168.10.100	192.168.10.1	192.168.10.2
Gate way	N/A	N/A	N/A
DNS	192.168.10.1	192.168.10.1	192.168.10.1

Thực hiện:

Bước 1: Mở Server Manager, click Manage → Add Roles and Features

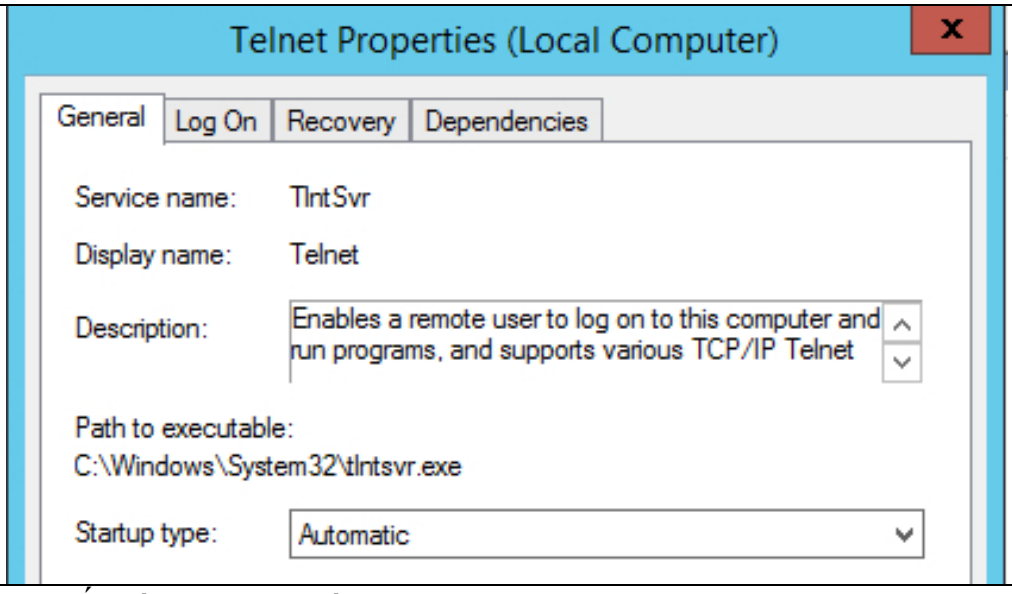


Bước 2:Hộp thoại Select Features → Group Policy Management và Telnet Server → Next

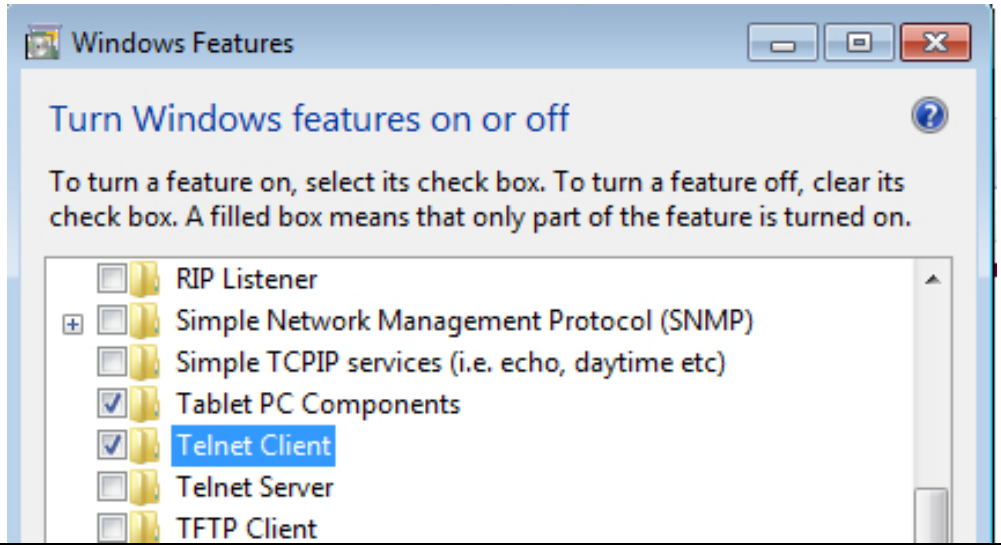
Add Roles and Features Wizard
Select features
DESTINATION SERVER
2k12-sv2.ntt.vn
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Select one or more features to install on the selected server.
Features
Description
Group Policy Management (Installed)
IIS Hostable Web Core
Ink and Handwriting Services
Internet Printing Client
.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect

Bước 3:Bật dịch vụ Telnet

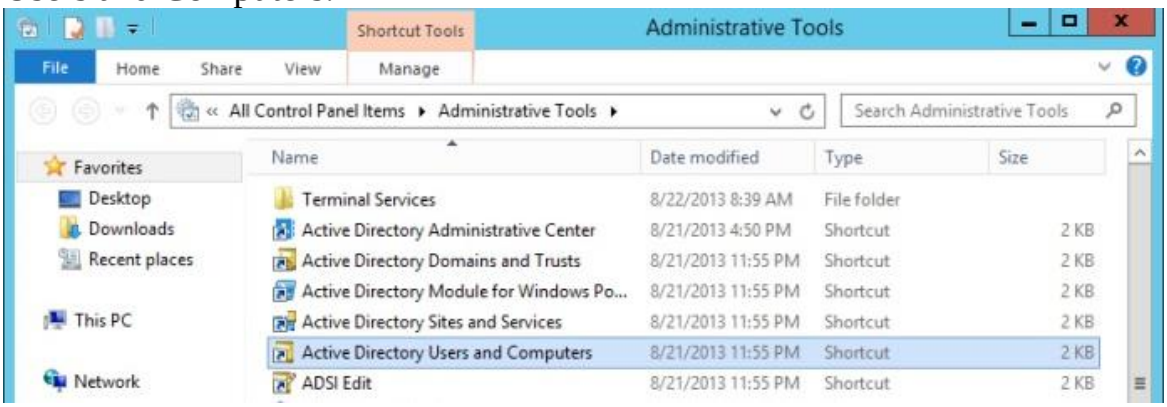
Start→Programs→Administrative Tools → Services. Click phải Telnet → Properties→Telnet Properties → Automatic → Apply→Telnet Properties → Start → Apply→ OK



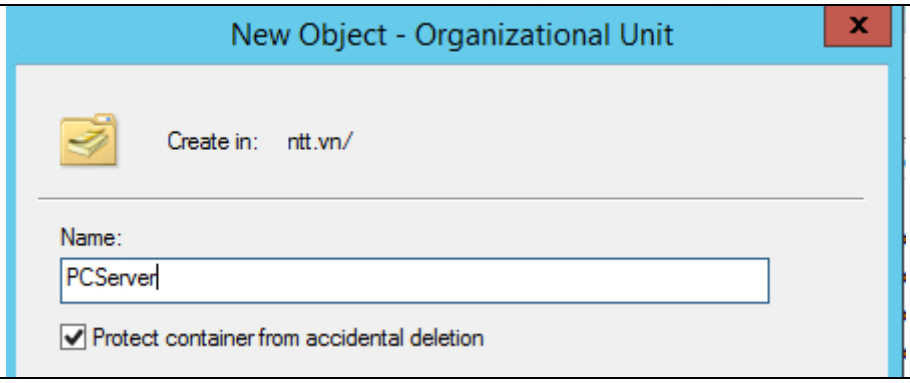
Bước 4:Cấu hình w7-c1 thành Telnet Client
Start → Settings→ Control Panel. Click phải Programs and Features → Open. →Programs and Features→ Turn Windows features on or off→Windows features → Telnet Client → OK


Windows Features
Turn Windows features on or off
To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.
RIP Listener
Simple Network Management Protocol (SNMP)
Simple TCPIP services (i.e. echo, daytime etc)
Tablet PC Components
Telnet Client
Telnet Server
TFTP Client

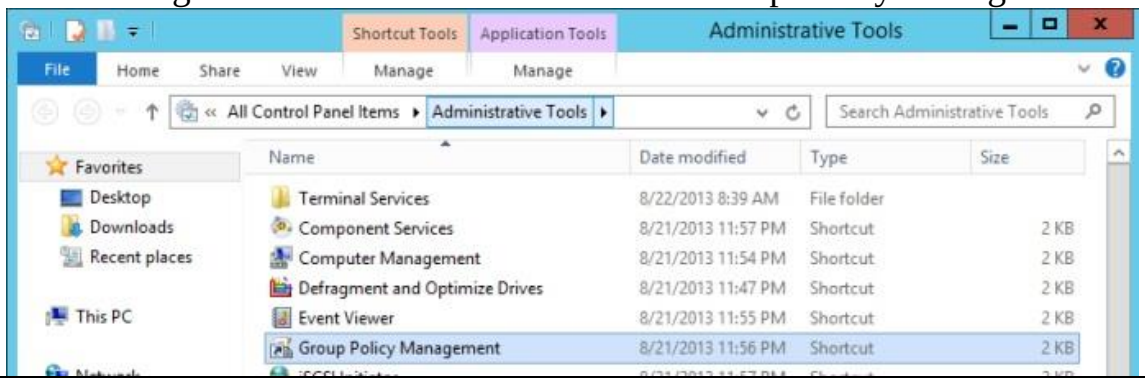
Bước 5: Start → Programs → Administrative Tools → Active Directory Users and Computers.



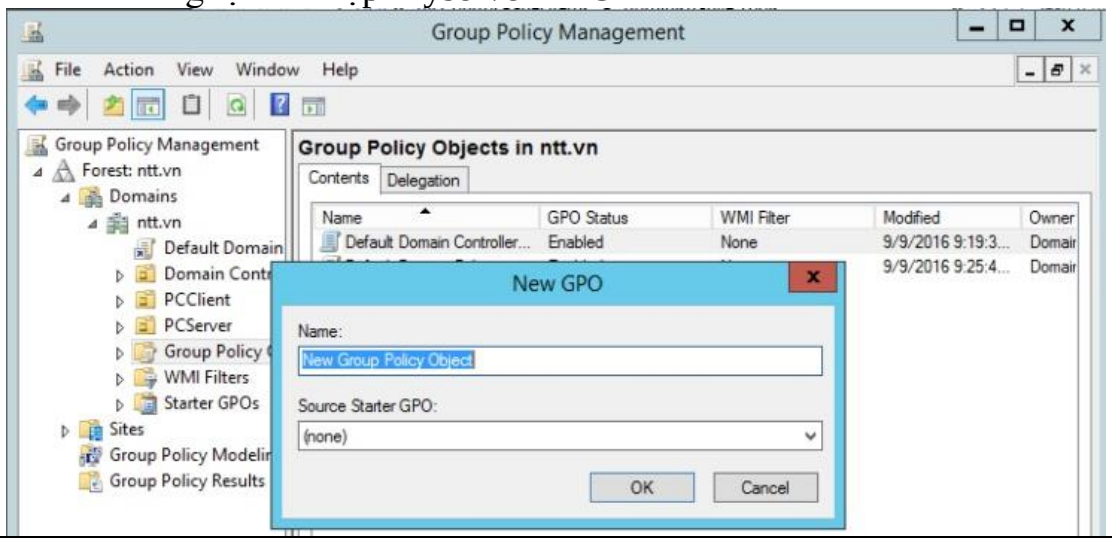
Bước 6:Hộp thoại New Object → Nhập PCServer → OK
Thao tác tương tự → Nhập PCClient → OK



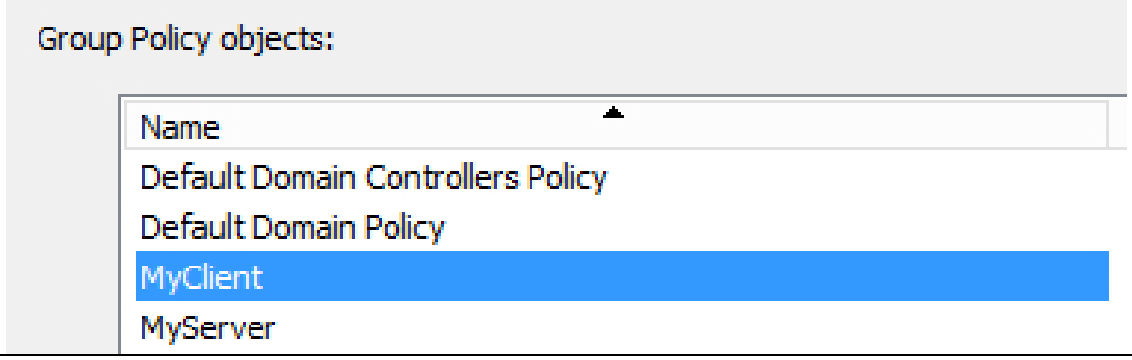
Bước 7:Tạo các Group Policy Object - GPO (thực hiện trên 2k12-sv2)
Start → Programs → Administrative Tools → Group Policy Management.



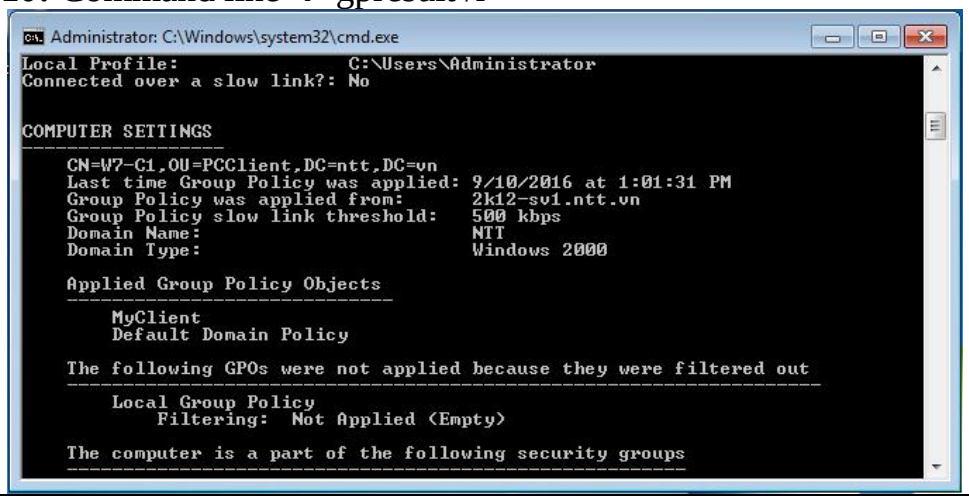
Bước 8: Group Policy Management → Click phải Group Policy Objects → New→ New GPO → Nhập MyClient → OK
Thao tác tương tự → Nhập Myserver → OK



Bước 9: Select GPO →MyClient → OK



Bước 10: Command line → gpresult /r


Administrator: C:\Windows\system32\cmd.exe
Local Profile: C:\Users\Administrator
Connected over a slow link?: No
COMPUTER SETTINGS
CN=W7-C1,OU=PCClient,DC=ntt,DC=vn
Last time Group Policy was applied: 9/10/2016 at 1:01:31 PM
Group Policy was applied from: 2k12-sv1.ntt.vn
Group Policy slow link threshold: 500 kbps
Domain Name: NTT
Domain Type: Windows 2000
Applied Group Policy Objects
MyClient
Default Domain Policy
The following GPOs were not applied because they were filtered out
Local Group Policy
Filtering: Not Applied (Empty)
The computer is a part of the following security groups

5. TÓM TẮT NỘI DUNG

- Xác định proxy và firewall
- Phân biệt proxy và firewall
- Triển khai proxy trong quản lý mail nội bộ và internet
- Triển khai firewall trong bảo mật hệ thống mạng

6. CÂU HỎI VÀ BÀI TẬP

CÂU HỎI

Câu 1: Thế nào là tấn công trên mạng. Trình bày các kiểu tấn công trên mạng.

Câu 2: Trình bày các cách triển khai bảo mật một hệ thống mạng.

Câu 3:Hãy nêu các thiết bị phần cứng và các giải pháp phần mềm để triển khai bảo mật hệ thống mạng. Thiết lập các chính sách;phân quyền cho user, hạn ngạch ổ đĩa, chính sách Password.

BÀI TẬP

Bài tập 1: Deploying Policies for Windows Firewall with Advanced Security trên Windows server 2008.

Yêu cầu: Cấu hình tường lửa và các hệ thống IPS nhằm tránh mọi sự tấn công nguy hiểm trên Internet. Một số tính năng mới của WFAS

Chuẩn bị:

- Một máy Windows Server 2008, đã nâng cấp thành Domain Controller (DC)
- Một máy Windows Server 2008, đã join domain
- Một máy Windows Vista, đã join domain
- Thiết lập thông số IP

Hướng dẫn làm bài

1.Cấu hình MBRSRV thành Telnet Server và cài đặt feature Group Policy Management

B1:Click phải Computer→ Manage→ Cửa sổ Server Manager → Click phải Features → Add Features

B2:Hộp thoại Select Features → chọn Group Policy Management và Telnet Server → Next

B3:Hộp thoại Confirm Installation Selections→ Install→ Hộp thoại Installation Results → Close

B4:Start → Programs → Administrative Tools → Services→ Click phải Telnet → Properties

B5:Hộp thoại Telnet Properties → chọn Automatic → Apply→ Hộp thoại Telnet Properties → chọn Start→ Apply → OK

2.Cấu hình CLIENT thành Telnet Client (thực hiện trên CLIENT)

B1: Start → Settings → Control Panel→ Click phải Programs and Features → Open

B2: Programs and Features → Chọn Turn Windows features on or off→ Windows features → Chọn Telnet Client → OK

3.Tạo các OU và di chuyển các Computer Account vào trong OU tương ứng (thực hiện trên máy DC)

B1: Start → Programs → Administrative Tools → Active Directory Users and Computers

B2: Tạo 2 OU→ Hộp thoại New Object → Nhập MyMemberServer → OK→ Quan sát kết quả

B3: Tạo các Group Policy Object_GPO

B4: Bật Firewall trên các máy CLIENT

Bài tập 2 : Cấu hình Firewall 2012 để quản lý mọi traffic vào ra của hệ thống
Yêu cầu: Cấu hình Firewall trên Windows Server 2012

Chuẩn bị: Một máy Windows Server 2012

Hướng dẫn làm bài
1.Thiết lập các cài đặt Firewall 2012

B1 : Từ giao diện Server Manager →Menu Tools→ Windows Firewall with Advanced Security.

B2 : Windows Firewall Properties, tính năng cho phép truy cập để sửa đổi các thiết lập cho ba chế độ firewall; Domain, Private và Public

2.Tùy chỉnh cho phép mức độ kiểm soát lưu lượng truy cập vào và ra máy chủ Windows Server 2012

B1: Server Manager từ thanh tác vụ→ menu Tools →Windows Firewall with Advanced Security

B2: Chọn một trong hai Inbound Rules hoặc Outbound Rules dưới Windows Firewall with Advanced Security

B3: Action bên phải của một trong hai Inbound Rules hoặc Outbound Rules → New Rule (cách mở port trên firewall)

B4: Chọn Port từ Rule Type Radial button → Next

B5: Tuỳ chọn loại giao thức trong protocol and Ports và bấm Next (*sử dụng giao thức TCP trên cổng 80 (HTTP).)*

B6: Click Allow the connection (Chọn một hành động để đưa vào phù hợp với lưu lượng truy cập) → Next.

B7: Check chọn cho phép firewall rule: Domain, Private, Public → Next.

B8: Ghi mô tả vào Name và Description → Finish.

B9: Sau khi tạo ra các rules sẽ được kích hoạt. Các quy tắc tường lửa được tìm thấy trên các tab Rule tương ứng,

BÀI 5: DANH SÁCH ĐIỀU KHIỂN TRUY CẬP

Mã bài MĐ 26-05

Thời gian: 14 giờ

I. MỤC TI ÊU: Sau khi học bài học này, sinh viên có khả năng

- Trình bày được khái niệm về danh sách truy cập
- Xác định được nguyên tắc hoạt động của danh sách truy cập
- Xác định được danh sách truy cập trong chuẩn mạng TCP/IP
- Thực hiện các thao tác an toàn với máy tính

II. NỘI DUNG CHÍNH

1. Khái niệm về danh sách truy cập

Mục tiêu **:** *Trình bày được khái niệm về danh sách truy cập*

1.1 Giới thiệu về điều khiển truy cập

Có ba khái niệm cơ bản trong mọi ngữ cảnh điều khiển truy cập, bao gồm:

+ Chính sách (policy): Là các luật do bộ phận quản trị tài nguyên đề ra.
+ Chủ thể (subject): Có thể là người sử dụng, mạng, các tiến trình hay các ứng dụng yêu cầu được truy cập vào tài nguyên.
+ Đối tượng (object): Là các tài nguyên mà chủ thể được phép truy cập.

1.2 Các kiểu xác thực

Có các kiểu xác thực các chủ thể được sử dụng phổ biến nhất:

+ Xác thực dựa trên cái người sử dụng biết (something you know).
+ Xác thực dựa trên những thứ người sử dụng có (something you have).
+ Xác thực dựa trên những thứ người sử dụng sở hữu bẩm sinh (something you are).
+ Xác thực dựa trên cái người sử dụng biết như mật khẩu (password), mật ngữ (pass phrase) hoặc mã số định danh cá nhân (PIN)…

1.3 Các nguy cơ và các điểm yếu của điều khiển truy cập

Phá mật khẩu (Password Cracking): Người quản trị hệ thống sẽ thiết lập các luật cho mật khẩu để đảm bảo người sử dụng tạo mật khẩu an toàn nhất. Kẻ tấn công có thể sử dụng kết hợp kỹ thuật tấn công Brute force và các thuật toán tinh vi để phá mật khẩu, truy cập vào hệ thống một cách bất hợp pháp. Các chính sách để đảm bảo mật khẩu đạt độ khó tránh bị phá bao gồm: mật khẩu phải tối thiểu 8 ký tự bao gồm chữ cái hoa, chữ cái thường, số và ký tự đặc biệt. Bên cạnh đó ý thức người sử dụng cũng cần được nâng cao như định kỳ nên thay đổi mật khẩu, đặt mật khẩu phải đạt độ khó nhưng dễ nhớ.

Chiếm quyền điều khiển (Heightened Access): Kẻ tấn công có thể khai thác các điểm yếu trên hệ điều hành, dùng công cụ để phá mật khẩu của người dùng và đăng nhập vào hệ thống trái phép, sau đó sẽ tiếp theo tìm cách nâng quyền truy cập ở mức cao hơn.

Social engineering: sử dụng sự ảnh hưởng và sự thuyết phục để đánh lừa người dùng nhằm khai thác các thông tin có lợi cho cuộc tấn công hoặc thuyết phục nạn nhân thực hiện một hành động nào đó. Social engineer (người thực hiện công việc tấn công bằng phương pháp social engineering) thường sử dụng điện thoại hoặc internet để dụ dỗ người dùng tiết lộ thông tin. Bằng phương pháp này, Social engineer tiến hành khai thác các thói quen tự nhiên của người dùng, hơn là tìm các lỗ hổng bảo mật của hệ thống.

1.4 Một số ứng tiêu biểu của điều khiển truy cập

Một số ứng dụng tiêu biểu của điều khiển truy cập như:

Kerberos: là hệ xác thực dựa trên nguyên lý mã hóa sử dụng khóa mật. Trong hệ Kerberos, một bên thứ ba được tin cậy cấp khóa phiên để bên người dùng và bên cung cấp dịch vụ có thể trao đổi thông tin với nhau trên mạng một cách an toàn. Đây là một công nghệ đã chín muồi và được sử dụng rộng rãi, tuy còn một số mặt hạn chế đang được tiếp tục khắc phục.

Đăng nhập một lần :(Single Sign On hay SSO) là giải pháp sử dụng một dịch vụ chứng thực trung tâm để chứng thực người dùng cho rất nhiều dịch vụ khác. Vì vậy, chỉ cần một tài khoản, khách hàng có thể đăng nhập và sử dụng rất nhiều dịch vụ chạy trên các máy chủ và tên miền khác nhau

Tường lửa: Firewall là một kỹ thuật được tích hợp vào hệ thống mạng để chống sự truy cập trái phép nhằm bảo vệ các tài nguyên mạng nội bộ cũng như hạn chế sự xâm nhập của một số thông tin không mong muốn. Cũng có thể hiểu rằng Firewall là một cơ chế để bảo vệ mạng tin tưởng (trusted network) khỏi các mạng không tin tưởng (untrusted network).

2. Nguyên tắc hoạt động của danh sách truy cập

Mục tiêu **:** *Xác định được nguyên tắc hoạt động của danh sách truy cập*

2.1 Điều khiển truy cập tùy quyền (DAC - Discretionary Access Control)

DAC hay còn gọi là mô hình điều khiển truy cập tùy quyền là một phương pháp nhằm hạn chế truy cập các đối tượng trên cơ sở nhận dạng và nhu cầu cần biết của nhiều người dùng và/hoặc của một nhóm các đối tượng trực thuộc. Phương pháp điều khiển truy cập được coi là tùy quyền là vì một chủ thể với một quyền truy cập nào đó có thể chuyển nhượng quyền truy cập (trực tiếp hay gián tiếp) sang bất cứ một chủ thể nào khác trong hệ thống.

2.1.1 Các khả năng (Capabilites)

Các khả năng tương ứng với các hàng của ma trận điều khiển truy cập. Khi phương pháp này được sử dụng, liên kết với mỗi tiến trình là một danh sách

các đối tượng có 12 thể được truy cập, cùng với một dấu hiệu của hoạt động nào được cho phép, nói cách khác, là miền của nó. Danh sách này được gọi là một danh sách các khả năng hoặc Clist và các thành phần trên đó được gọi là những khả năng.

2.1.2 Các hồ sơ (Profiles)

Profiles được triển khai trên nhiều dạng hệ thống, sử dụng một danh sách bảo vệ đối tượng kết hợp với từng người dùng. Nếu một người dùng được truy cập đến nhiều đối tượng được bảo vệ, profiles có thể rất lớn và khó quản lý. Viêc tạo, xóa và thay đổi truy cập đến đối tượng được bảo vệ yêu cầu nhiều thao tác khi nhiều profile của người dùng phải được cập nhật. Việc xóa một đối tượng có thể yêu cầu một vài thao tác xác định một người dùng có các đối tượng ở trong profile của mình. Với profile, để trả lời câu hỏi "ai có quyền truy cập vào đối tượng được bảo vệ" là rất khó. Nhìn chung, không nên triển khai profiles trong hệ thống DAC

2.1.3 Access control lists (ACLs)

Danh sách điều khiển truy cập (Access control lists – ACLs) là danh sách mô tả việc liên kết các quyền truy nhập của người dùng với mỗi đối tượng. Đó là một danh sách có chứa tất cả các miền có thể truy cập vào các đối tượng. Thông thường trong các tài liệu bảo mật, người dùng được gọi là các chủ thể (subject), để tương ứng với những thứ họ sở hữu, các đối tượng, chẳng hạn như các file. Mỗi tập tin có một bản ghi ACL liên kết với nó. ACL không thay đổi nếu người dùng khởi động một tiến trình hoặc 100 tiến trình. Quyền truy nhập được gán cho chủ sở hữu, không phải gán trực tiếp cho tiến trình.

2.1.4 Các bit bảo vệ (Protection bits)

Các bit bảo vệ đặc trưng ma trận điều khiển truy cập theo cột. Trong cơ chế "bit bảo vệ" trên các hệ thống như UNIX, bit bảo vệ cho mỗi đối tượng được sử dụng thay vì liệt kê danh sách người dùng có thể truy cập vào đối tượng. Trong UNIX các bit bảo vệ chỉ ra hoặc mọi người, nhóm đối tượng hoặc người sở hữu mới có các quyền để truy cập đến đối tượng được bảo vệ. Người tạo ra đối tượng được gọi là chủ sở hữu (owner), chủ sở hữu này có thể thay đổi bit bảo vệ. Hệ thống không thể cho phép hay không cho phép truy cập tới một đối tượng được bảo vệ trên bất kỳ người dùng nào

2.1.5 Mật khẩu

Mật khẩu bảo vệ các đối tượng đại diện cho ma trận kiểm soát truy cập của hàng. Nếu mỗi người sử dụng sở hữu mật khẩu của mình cho từng đối tượng, sau đó mật khẩu là một vé cho đối tượng, tương tự như một hệ thống khả năng. Trong hầu hết các cài đặt thực hiện bảo vệ mật khẩu, chỉ có một mật khẩu cho mỗi đối tượng hoặc mật khẩu mỗi đối tượng cho mỗi chế độ truy cập tồn tại.

2.2 Các giải pháp đảm bảo an ninh, an toàn dựa trên điều khiển truy cập

2.2.1 Các chính sách quản trị người dùng an toàn

Tài khoản phải được bảo vệ bằng mật khẩu phức hợp (độ dài mật khẩu, độ khó mật khẩu). − Chủ sở hữu tài khoản chỉ được cung cấp quyền hạn truy cập thông tin và dịch vụ cần thiết (không thiếu quyền hạn mà cũng không thể để thừa).

Mã hóa tài khoản trong giao dịch trên mạng (kể cả giao dịch trong mạng nội bộ).

Lưu trữ tài khoản an toàn (nhất định cơ sở dữ liệu lưu giữ tai khoản phải được đặt trên những hệ thống an toàn và được mã hóa).

Những người tạo và quản lý tài khoản (đặc biệt là những tài khoản hệ thống và tài khoản vận hành, kiểm soát các dịch vụ) cho toàn bộ tổ chức là những người được xem là tin cậy tuyệt đối.

Đình chỉ hoạt động những tài khoản tạm thời chưa sử dụng, xóa những tài khoản không còn sử dụng.

Tránh việc dùng chung mật khẩu cho nhiều tài khoản.

Khóa tài khoản sau một số lần người sử dụng đăng nhập không thành công vào hệ thống.

Có thể không cho phép một số tài khoản quản trị hệ thống và dịch vụ, không được đăng nhập từ xa, vì những hệ thống và dịch vụ này rất quan trọng và thông thường chỉ cho phép được kiểm soát từ bên trong (internal network), nếu có nhu cầu quản trị và hỗ trợ từ xa người quản trị vẫn dễ dàng thay đổi chính sách để đáp ứng nhu cầu.

2.2.2 Một số biện pháp đảm bảo an ninh, an toàn dựa trên điều khiển truy cập cho các ứng dụng và các dịch vụ

Dưới đây sẽ là một số chính sách được khuyến nghị đảm bảo an toàn cho các máy chủ ứng dụng và dịch vụ:

Đặt các máy chủ trong vùng DMZ. Thiết lập firewall không cho các kết nối tới máy chủ trên toàn bộ các cổng, ngoại trừ được sử dụng cho các dịch vụ và ứng dụng mà máy chủ sử dụng. Loại bỏ toàn bộ các dịch vụ không cần thiết khỏi máy chủ (chỉ giữ lại nếu thật cần thiết). Mỗi dịch vụ không cần thiết sẽ bị lợi dụng để tấn công hệ thống nếu không có chế độ bảo mật tốt.

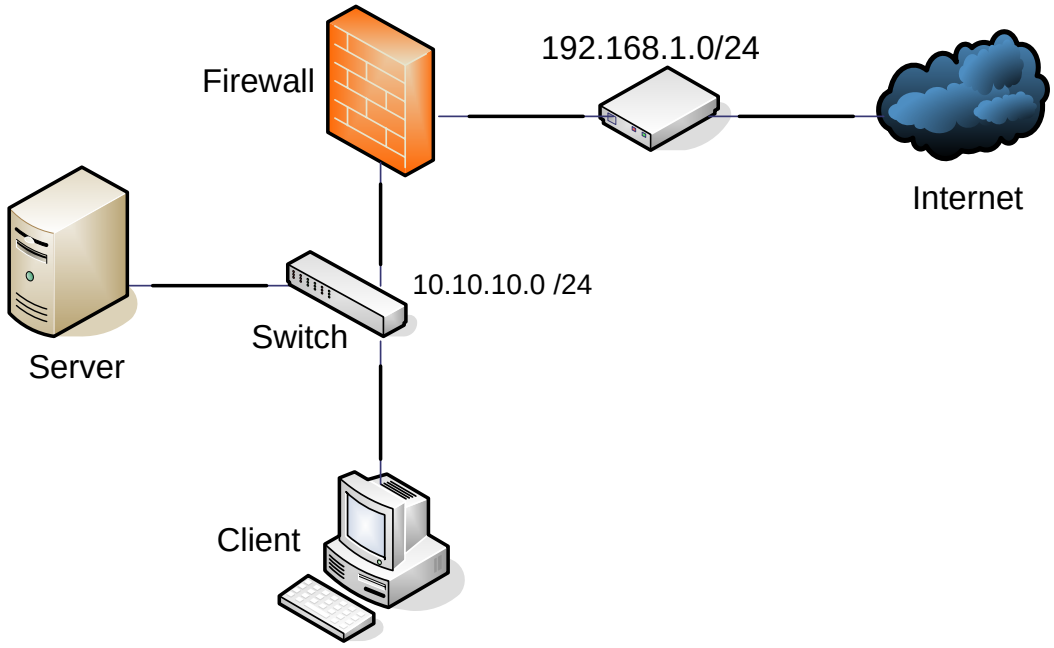
Không cho phép quản trị hệ thống từ xa, trừ khi nó được đăng nhập theo kiểu mật khẩu chỉ sử dụng một lần hay đường kết nối đã được mã hoá.

Giới hạn số người có quyền quản trị hay truy cập mức tối cao (root).

Tạo các log file theo dõi hoạt động của người sử dụng và duy trì các log file này trong môi trường được mã hoá.

3.Bài tập thực hành

Bài tập 1 :cho mô hình mạng như sau :



Yêu cầu: Cài đặt, cấu hình điều khiển truy cập an toàn cho các ứng dụng và dịch vụ.

Chuẩn bị :

- 1 máy PC cài win2k3→ nâng lên DC
- 1 máy PC cài win2k3→cài ISA 2006→ kết nối internet
- 1 máy PC cài winxp
- 1 switch
- 1 router kết nối internet
- 3 sợi cáp mạng bấm thẳng
- Đấu nối theo mô hình
- Thiết lập đia chỉ IP và đấu nối mô hình mạng

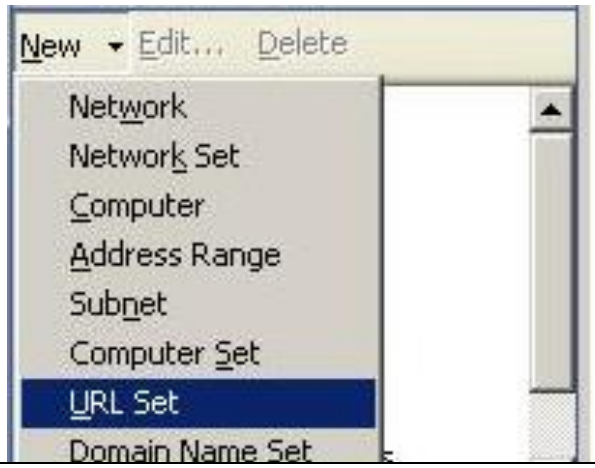
Thực hiện:

1.Cấu hình truy cập web nội bộ và cấm tải file có đuôi .exe

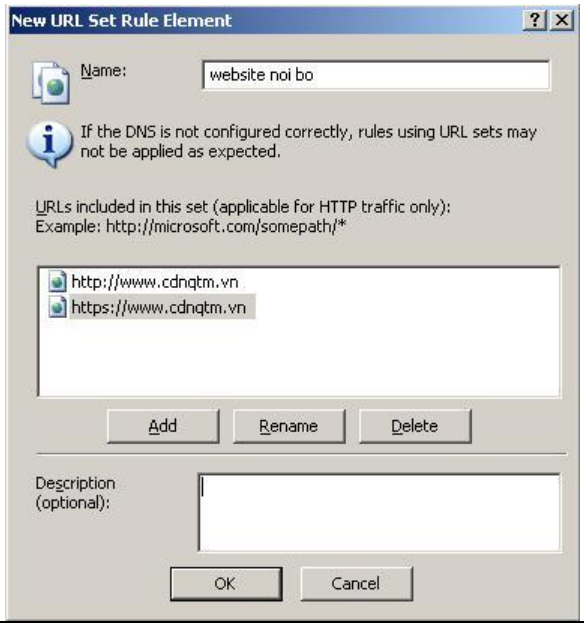
Bước 1 : Tạo rule ping cho phép nội bộ ping đến máy isa→ Tạo rule cho phép truy cập internet

Cấu hình cho phép truy cập website nội bộ. Tạo đường dẫn website

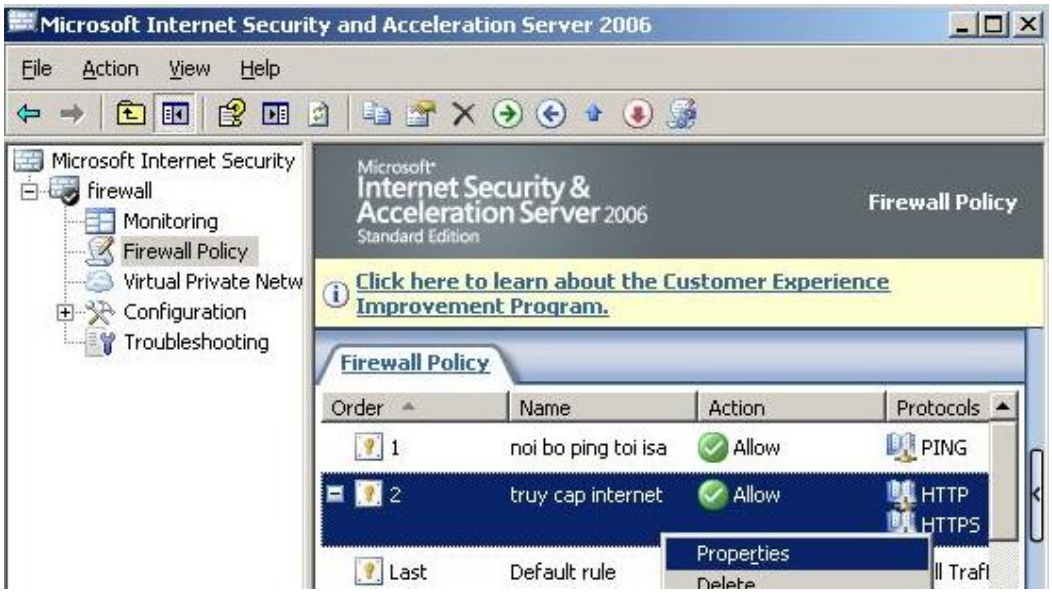
Tại Toolbox → network object → new → URL Set



Bước 2 : Đặt tên và nhập tên trang web nội bộ vào → OK

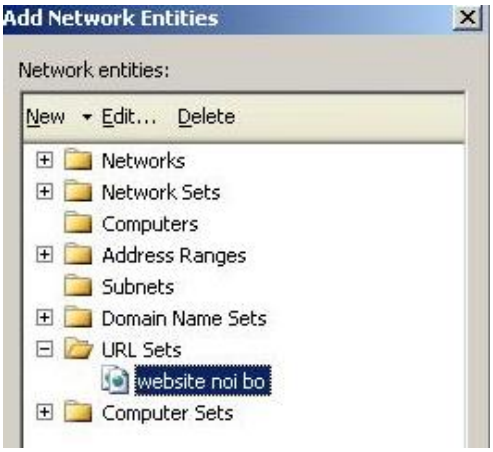


Bước 3 : Click phải chuột lên rule "truy cap internet" → Properties



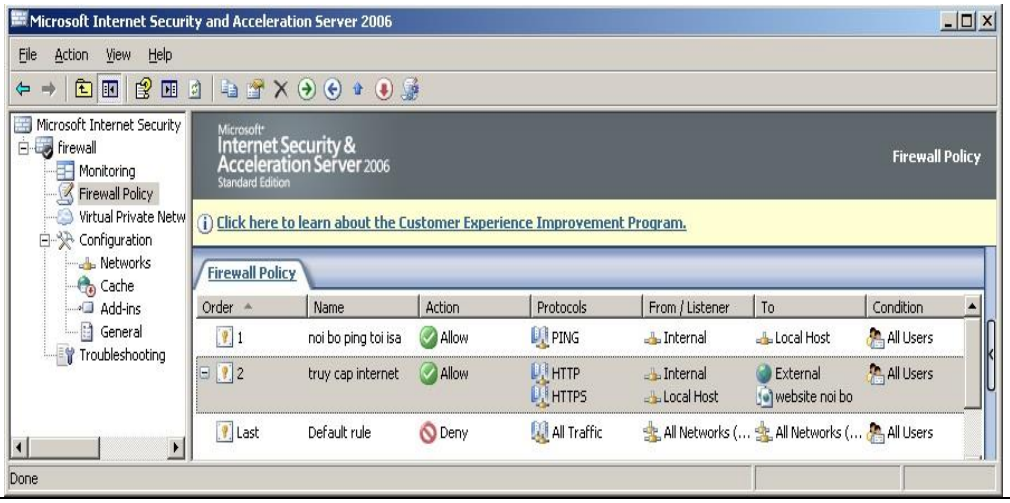
Kế tiếp→ Tab To → Add

Bước 4 : Chọn URL Sets → chọn tên vừa đặt ở trên

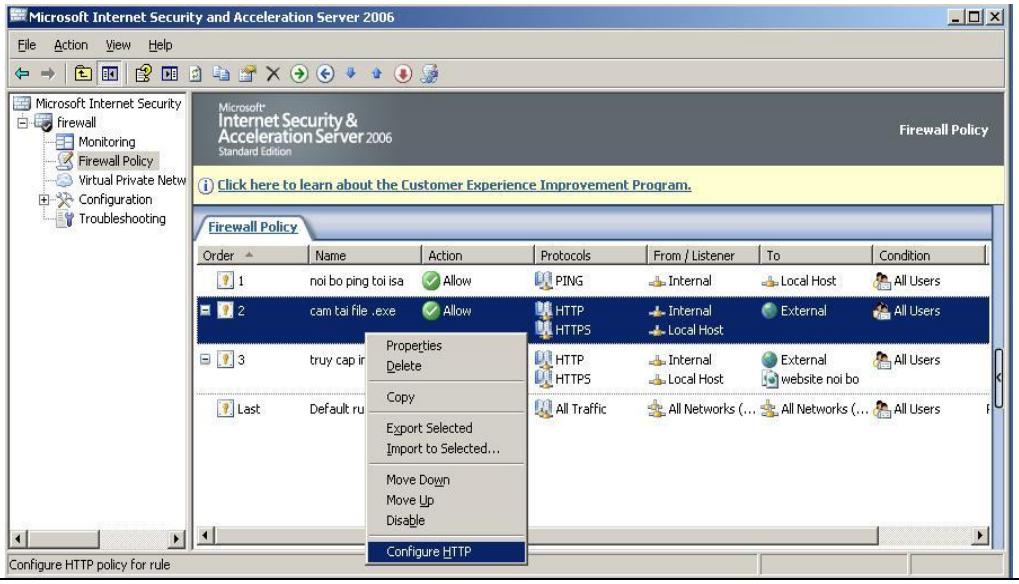


Chọn OK → sau đó chọn Apply

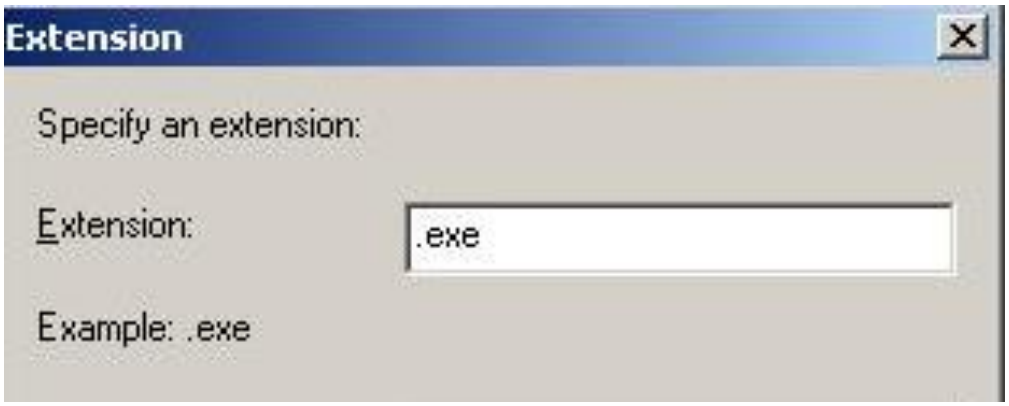
Bước 5 : Như vậy tạo xong rule truy cập website nội bộ



Bước 6 : Tạo rule cho phép truy cập internet , nhưng cấm tải những file, hoặc các ứng dụng có kiểu file .exe→Click phải lên rule "cam tai file .exe" → Configure HTTP



Bước 7 : Chọn Tab Extensions → Block specified extensions (allow all other) → Add



Kế tiếp→ Nhập ".exe" → OK→OK

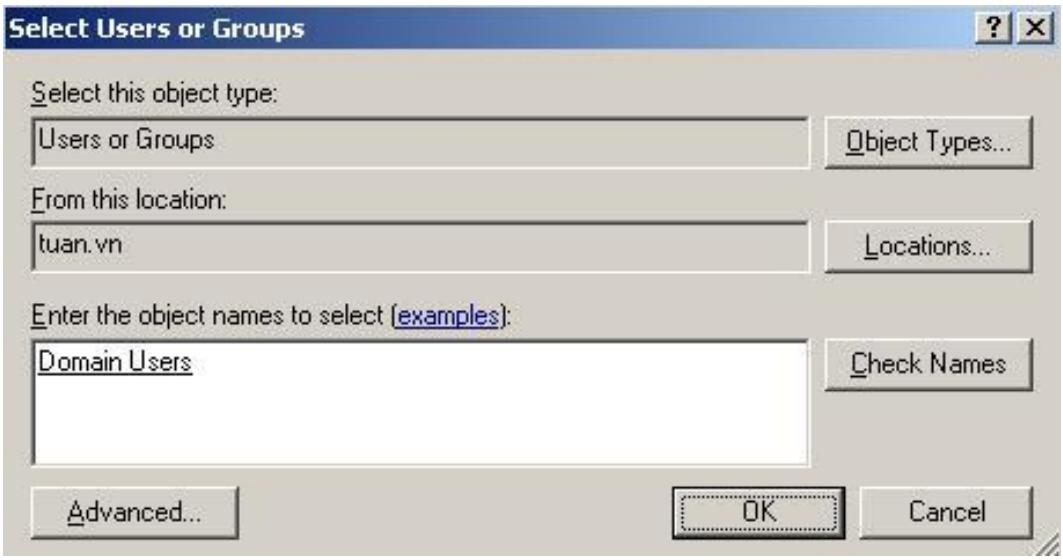
Bước 8 : Chọn Apply, sau đó thử tải file có đuôi .exe

2.Cấu hình giới hạn đường truyền

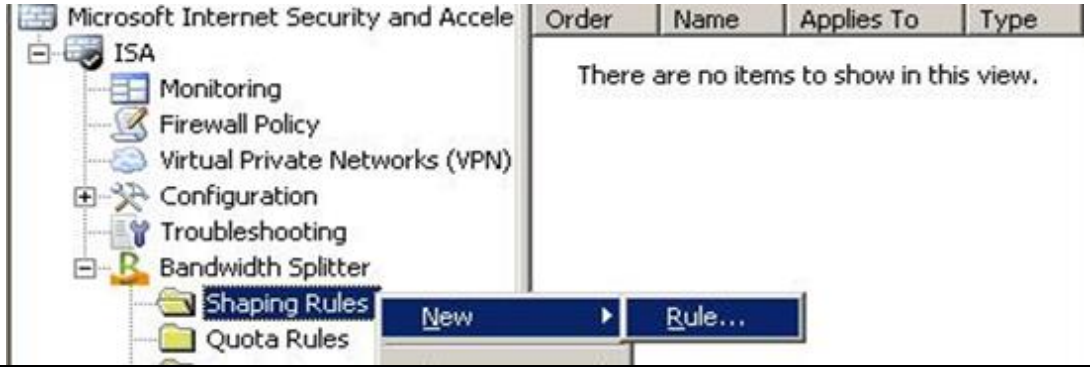
Bước 1 : Tại Toolbox → user→ New→ Nhập tên → next

Chọn add → windows user→ location→ Chọn tên domain →OK

Bước 2 : Nhập domain users →check name



Kế tiếp→Next→ Finish→ Chọn apply

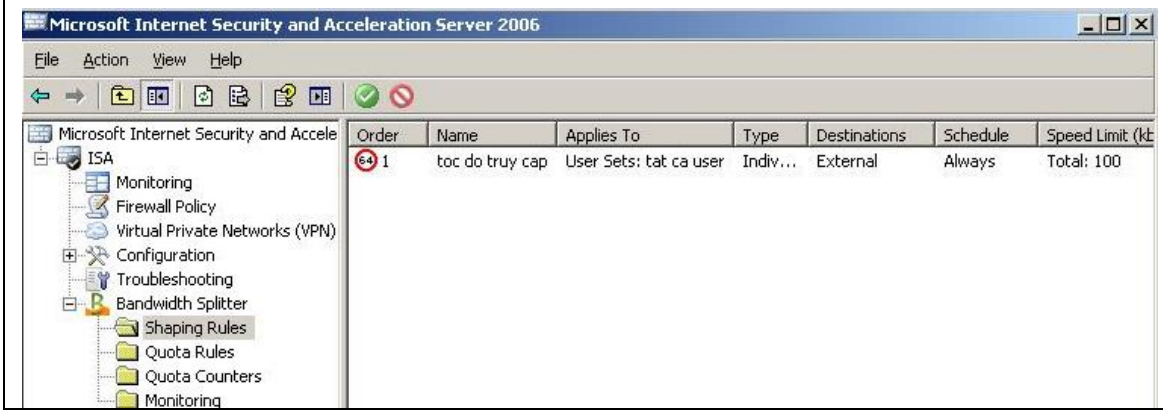


Bước 4: Chọn user → add→Chọn tên vừa tạo ở trên → add → close→Next→Add

Bước 5 : Chọn external → add → close→Next→Next

Đường truyền 1MB và có tổng cộng 10 user thì lấy 1mb chia cho 10 như vậy mỗi user được 100kb→nhập 100kb→next

Bước 6 : Bỏ check chọn →Next→Next→Next →Hoàn tất cấu hình→ Finish



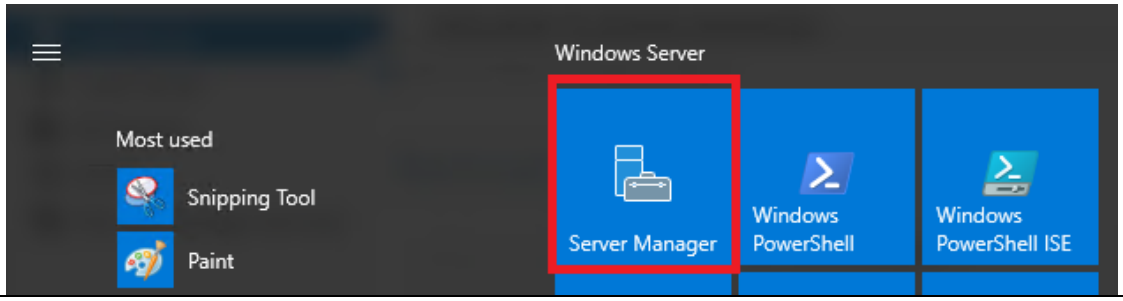
Bài tập 2 : Các role và Features mặc định không được cài đặt cùng Windows, muốn cài đặt chúng, người dùng phải dùng Server Manager để tiến hành cài đặt.

Yêu cầu : Cài đặt, tháo gỡ Roles và Features trên Windows Server 2012/2016

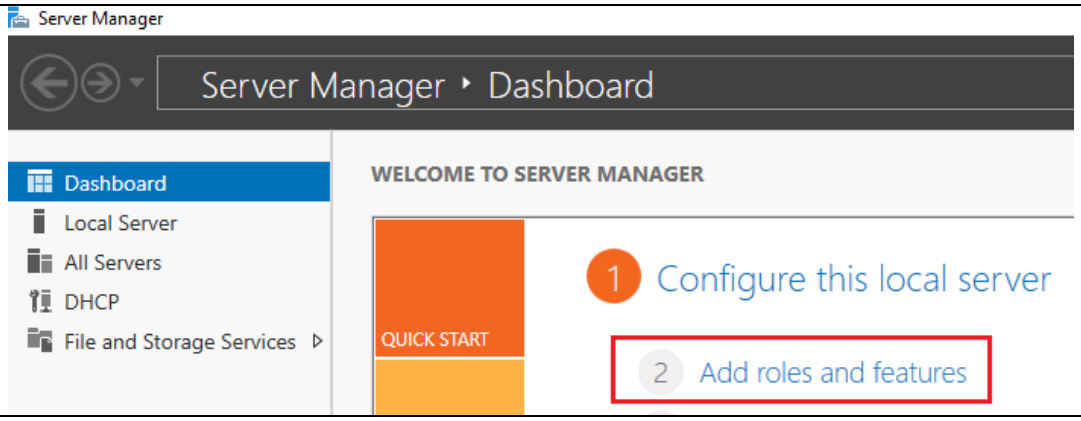
Chuẩn bị: 1 máy PC cài win server 2012/2016

Thực hiện

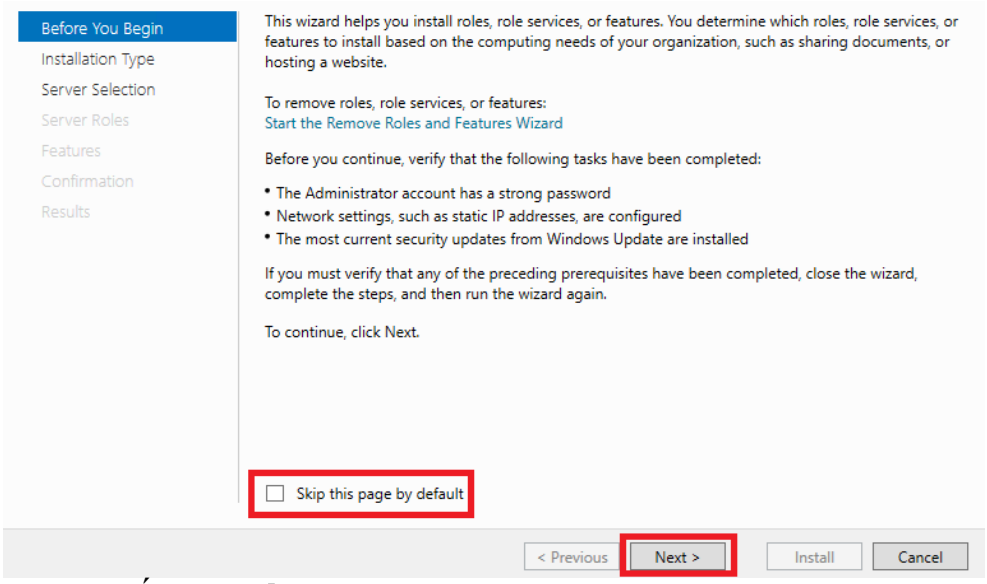
Bước 1: Giao diệnServer Manager



Bước 2: Cài đặt Roles và Features:Từ Dashboard của Server Manager→Add roles and features.

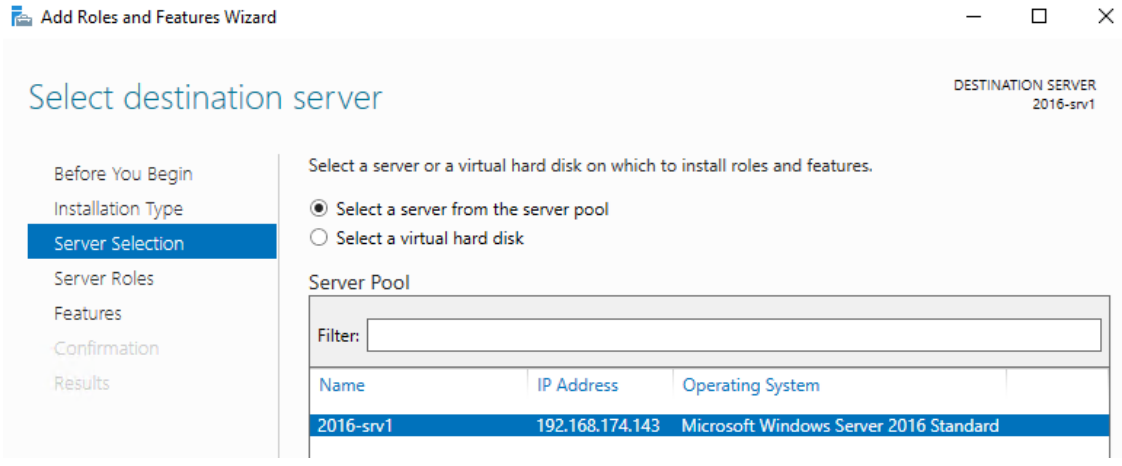


Bước 3: vào Add Roles and Features Wizard→ Before you begin→ Skip this page by default.

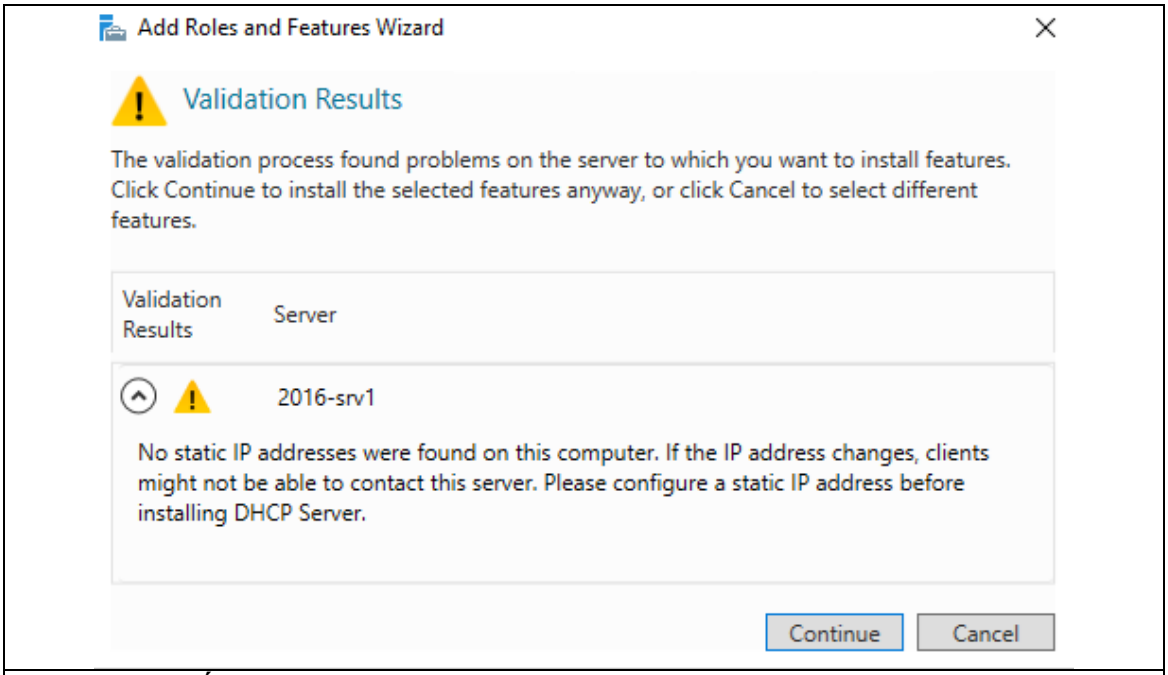

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.
To remove roles, role services, or features:
Start the Remove Roles and Features Wizard
Before you continue, verify that the following tasks have been completed:
• The Administrator account has a strong password
• Network settings, such as static IP addresses, are configured
• The most current security updates from Windows Update are installed
If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.
To continue, click Next.
Skip this page by default
< Previous
Next >
Install
Cancel

Tiếp theo →Role-based or feature-based installation

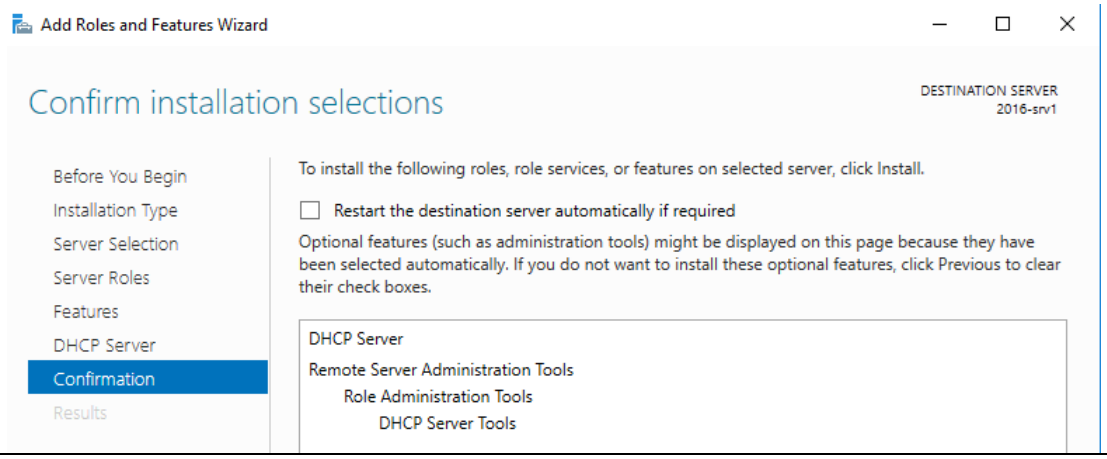
Bước 4: Cài đặt Roles và Features→ Server Roles→ Roles→Next



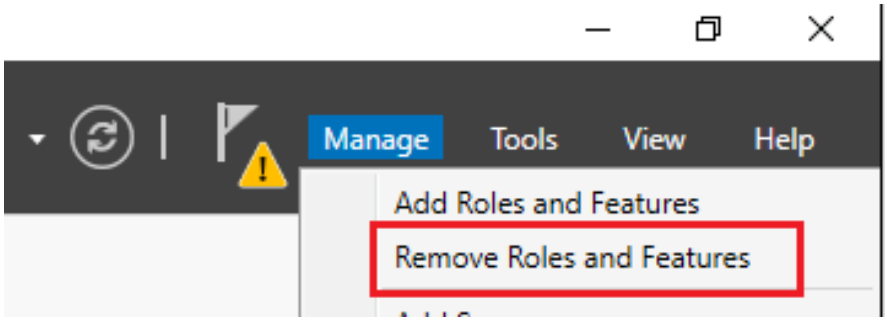
Bước 5: Thiết lập Ip tĩnh→ thêm các Feature hỗ trợ tương tự như Role


Add Roles and Features Wizard
Validation Results
The validation process found problems on the server to which you want to install features. Click Continue to install the selected features anyway, or click Cancel to select different features.
Validation Results
Server
2016-srv1
No static IP addresses were found on this computer. If the IP address changes, clients might not be able to contact this server. Please configure a static IP address before installing DHCP Server.
Continue
Cancel

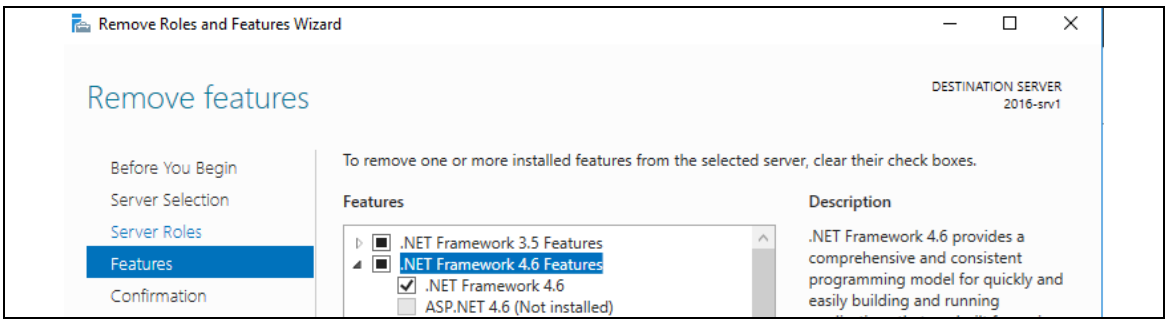
Bước 6: Xuất hiện các thông tin của Role hoặc Feature đã chọn cài đặt→Tiếp theo, trong của sổ Confirm installation selections→ Restart the destination server automatically if requiered


Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
2016-srv1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DHCP Server
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
DHCP Server
Remote Server Administration Tools
Role Administration Tools
DHCP Server Tools

Bước 7: Tháo gỡ Roles và Features→Trong Server Manager → Manage chọn Remove Roles and Features



Bước 8:chọn Roles và Features cần gỡ bỏ


Remove Roles and Features Wizard
Remove features
DESTINATION SERVER
2016-srv1
Before You Begin
Server Selection
Server Roles
Features
Confirmation
To remove one or more installed features from the selected server, clear their check boxes.
Features
Description
.NET Framework 3.5 Features
.NET Framework 4.6 Features
.NET Framework 4.6
ASP.NET 4.6 (Not installed)
.NET Framework 4.6 provides a comprehensive and consistent programming model for quickly and easily building and running

4- TÓM TẮT NỘI DUNG

- Điều khiển truy cập là một trong các biện pháp quan trọng nhằm đảm bảo an ninh, an toàn cho thông tin, hệ thống và mạng.
- Điều khiển truy cập thuộc lớp các biện pháp ngăn chặn tấn công, đột nhập
- Các giải pháp đảm bảo an ninh, an toàn hiệu quả cho các ứng dụng dựa trên điều khiển truy cập
- DAC cho phép kiểm soát truy cập thực hiện được đối với object dựa trên cơ sở cho phép hoặc từ chối hoặc cả hai do một user riêng biệt, thường do người sở hữu object đó quyết định. MAC cho phép việc kiểm soát truy cập dựa vào nhãn bảo mật gửi kèm tới các user (chính xác hơn là chủ thể) và object.
- Kiểm soát truy nhập dựa trên luật cho phép người dùng truy nhập vào hệ thống vào thông tin dựa trên các luật (rules) đã được định nghĩa trước. Firewalls/Proxies là ví dụ điển hình về kiểm soát truy nhập dựa trên luật:
  - ➢ Dựa trên địa chỉ IP nguồn và đích của các gói tin.
  - ➢ Dựa trên phần mở rộng các files để lọc các mã độc hại.
  - ➢ Dựa trên IP hoặc các tên miền để lọc/chặn các website bị cấm.
  - ➢ Dựa trên tập các từ khoá để lọc các nội dung bị cấm

5- CÂU HỎI VÀ BÀI TẬP

CÂU HỎI

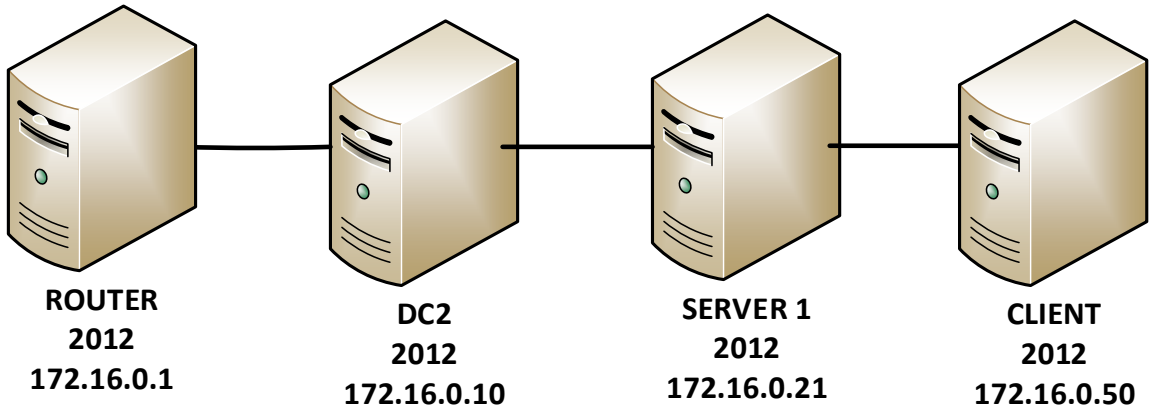
Câu 1 : Trình bày một chính sách truy cập quyền sở hữu tập tin và dữ liệu (*File and data ownership*)

Câu 2 : Trình bày điều khiển truy cập dùng chính sách (*rule-based access control*)

Câu 3 : Trình bày bốn mô hình điều khiển truy cập chính**.**

BÀI TẬP

Bài tập 1: Cho mô hình mạng



Yêu cầu: Cấu hình Direct Access trên Windows Server 2012 (vi-VN)

Chuẩn bị:

- DC2012: *Domain Controller* chạy Windows Server 2012 (domain mcthub.local)
- SERVER1: Domain Member đảm nhận vài trò *Network Location Server (NLS)* chạy Windows Server 2012. Đây là Server giúp các Direct Access Client xác định vị trí của nó. Nếu Direct Access Client liên lạc được với Network Location Server thì Direct Access Client xác định nó đang ở trong mạng nội bộ và sử dụng DNS của hệ thống để phân giải.
- ROUTER**:** Domain Member đảm nhận vai trò *Direct Access Server* chạy Windows Server 2012
- CLIENT1: Domain Member chạy Windows 8.
- Đặt thông số TCP/IP card Internal cho các máy tính theo bảng sau đây

ROUTER	DC2012	SERVER1	CLIENT1
IP:172.16.0.1 Subnet Mask: 255.255.0.0 Default Gateway (trống) DNS:172.16.0.10	IP:172.16.0.10 Subnet Mask: 255.255.0.0 Default Gateway 172.16.0.1 DNS: 172.16.0.10	IP:172.16.0.21 Subnet Mask: 255.255.0.0 Default Gateway 172.16.0.1 DNS:172.16.0.10	IP:172.16.0.50 Subnet Mask: 255.255.0.0 Default Gateway 172.16.0.1 DNS:172.16.0.10

Hướng dẫn làm bài

1.Cài đặt và cấu hình CA Server

B1: Trên máy DC2012, mở Server Manager và cài đặt dịch vụ Active Directory Certificate Service.

B2 : Chọn Server cần cài đặt là DC2012.mcthub.local→Active Directory Certificate Service.

B3: cài thêm các Feature →Install

B4: Configure Active Directory Certificate Service on the desstination server để thực hiện thao tác cấu hình cho dịch vụ.

B5 : User Account dùng để cấu hình là MCTHUB\Administrator→Chọn loại CA là Enterprise CA

B6: Configure →Close → restart các máy ROUTER, SERVER1 và CLIENT1 để các máy này tự động trust CA Server trên máy DC2012

2.Cài đặt Web Server (IIS) và chuẩn bị CRL Distribution Point trên Direct Access Server

B1: Trên máy ROUTER, tạo sẵn 1 thư mục tên tùy ý (ví dụ **C:\CRLD**), thư mục này sẽ chứa Certificate Revocation List (CRL) được publish từ CA Server.

B2: cài đặt Web Server (IIS)→ ROUTER.mcthub.local →Web Server (IIS)→ Install →Close

B3: Mở IIS Console cấu hình nơi chứa CRL (CRLs Distribution Point)→ Virtual Directory→C:\CRLD→share thư mục C:\CRLD

B4: Đưa máy DC2012 vào danh sách phân quyền (Access Control List) và phân quyền Full Control cho Everyone và DC2012 →OK

4.Publish CRL

B1: DC2021 (CA Server)→ Certification Authority→Publish CRL và Delta CRL sang Direct Access Server (ROUTER)

B2: Tab Extensions→Add →CRL Distribution Point (CDP)→ nhập http://CRL.mcthub.local/CRLD/ → <CAName> → Insert

B3: Variable →<CRLNameSuffix> → <DeltaCRLAllowed> → Insert→OK

5.CA Server - Tạo và phát hành Certificate Template cho Network Location Server & Direct Access Server

B1: Chọn Certificate Template Web Server và sao chép Certificate Template này thành một Certificate Template mới

B2Sang tab Request Handling đánh dấu check Allow private key to be exported để có thể Export Certificate đề phòng trường hợp bị mất Certificate

B3: Sang Tab Security, phân quyền Enroll cho group Authenticated Users. Nhấn nút OK để xác nhận tạo Certificate Templates mới

B4: Certificate Templates Network Location Server Certificate đã tạo trước đó → OK

Bài tập 2: NIC Teaming cho phép 2 hoặc nhiều NIC vật lý (Network Interface Card) liên kết với nhau, tạo thành 1 NIC logic có khả năng LoadBalancing và tăng HA (High Availability) cho hệ thống.

Yêu cầu: Cấu hình NIC Teaming trên Windows Server 2012

Chuẩn bị: Windows Server 2012 – 4 NICs

Hướng dẫn làm bài

B1 : Server manager →Local Server → Diasbled → NIC →TEAMS →TASKS → New Team

B2 : LACP : giao thức để tạo EthernetChanel →OK→Network Connections sẽ xuất hiện 1 "NIC mới"

B3 : NIC Ethernet 2 →chọn Properties : Ta thấy rằng mọi chức năng của NIC này đều được loại bỏ – ngoại từ 1 Protocol dùng để tạo NIC Teaming

B4: NIC Team1 →Properties : ta thấy rằng nó đã trở thành 1 NIC thực thụ, và mọi cấu hình IP,DNS và những mục liên quan NIC ta sẽ đều cấu hình tại đây

B5 : Configure NIC Teaming→NIC mới → phải chuột chọn Add to Team "Tên team cần thêm"

B6 : ping -t 1 server khác cùng mạng→Cấu hình 3 NIC – với NIC 1(Ethernet) và 2 (Ethernet 2) ở trạng thái Active, NIC 3 (Ethernet 4) ở trạng thái Standby

B7 : Cho NIC 1 disconnect (trạng thái Faulted), ngay lập tức, NIC 3 trở thành ACtive.

BÀI 6 :VIRUS VÀ CÁCH PHÒNG CHỐNG

Mã bài MĐ 26-06

Thời gian :5 giờ

I. MỤC TIÊU: Sau khi học bài học này, sinh viên có khả năng

- Xác định được virus máy tính
- Trình bày được cách thức lây lan của virus máy tính
- Phân biệt được các loại virus
- Phòng ngừa được sự xâm nhập của virus.
- Thực hiện các thao tác an toàn với máy tính

II. NỘI DUNG CH ÍNH

1. Giới thiệu tổng quan về virus

Mục tiêu : Xác định được virus máy tính

1.1.Virus là gì ?

Thuật ngữ virus tin học dùng để chỉ một chương trình máy tính có thể tự sao chép chính nó lên nơi khác (đĩa hoặc file) mà người sử dụng không hay biết. Ngoài ra, một đặc điểm chung thường thấy trên các virus tin học là tính phá hoại, nó gây ra lỗi thi hành, thay đổi vị trí, mã hoá hoặc huỷ thông tin trên đĩa.

1.2 Các khái niệm có liên quan

Sâu máy tính (*worm*): là các chương trình cũng có khả năng tự nhân bản tự tìm cách lan truyền qua hệ thống mạng (thường là qua hệ thống thư điện tử). Điểm cần lưu ý ở đây, ngoài tác hại thẳng lên máy bị nhiễm, nhiệm vụ chính của worm là phá các mạng (*network*) thông tin, làm giảm khả năng hoạt động hay ngay cả hủy hoại các mạng này. Nhiều nhà phân tích cho rằng worm khác với virus, họ nhấn mạnh vào đặc tính phá hoại mạng nhưng ở đây worm được coi là một loại virus đặc biệt..

2. Cách thức lây lan và phân loại virus

Mục tiêu : Trình bày được cách thức lây lan của virus máy tính

2.1 B-Virus

2.1.1 Kỹ thuật kiểm tra tính duy nhất

Virus phải tồn tại trong bộ nhớ cũng như trên đĩa, song sự tồn tại quá nhiều bản sao của chính nó trên đĩa và trong bộ nhớ sẽ chỉ làm chậm quá trình Boot máy, cũng như chiếm quá nhiều vùng nhớ ảnh hưởng tới việc tải và thi hành các chương trình khác đồng thời cũng làm giảm tốc độ truy xuất đĩa. Chính vì thế, kỹ thuật này là một yêu cầu nghiêm ngặt với B-virus.

2.1.2 Kỹ thuật lưu trú

Sau khi thực hiện xong chương trình POST, giá trị tổng số vùng nhớ vừa được Test sẽ được lưu vào vùng BIOS Data ở địa chỉ 03h. Khi hệ điều hành nhận quyền điều khiển, nó sẽ coi vùng nhớ mà nó kiểm soát là giá trị trong địa chỉ này. Vì vậy để lưu trú, mọi B-Vius đều áp dụng kỹ thuật này.

2.1.3 Kỹ thuật lây lan

Đoạn mã thực hiện nhiệm vụ lây lan là đoạn mã quan trọng trong chương trình virus. Để đảm bảo việc lây lan, virus khống chế ngắt quan trọng nhất trong việc đọc/ghi vùng hệ thống: đó là ngắt 13h, tuy nhiên để đảm bảo tốc độ truy xuất đĩa, chỉ các chức năng 2 và 3 (đọc/ghi) là dẫn tới việc lây lan.

2.1.4 Kỹ thuật ngụy trang và gây nhiễu

Kỹ thuật này ra đời khá muộn về sau này, do khuynh hướng chống lại sự phát hiện của người sử dụng và những lập trình viên đối với virus. Vì kích thước của virus khá nhỏ bé cho nên các lập trình viên hoàn toàn có thể dò từng bước xem cơ chế của virus hoạt động như thế nào, cho nên các virus tìm mọi cách lắt léo để chống lại sự theo dõi của các lập trình viên.

2.1.5 Kỹ thuật phá hoại

Căn cứ vào thời điểm phá hoại, có thể chia ra thành hai loại:

Loại định thời: Loại này lưu giữ một giá trị, giá trị này có thể là ngày giờ, số lần lây nhiễm, số giờ máy đã chạy, ... Nếu giá trị này vượt quá một con số cho phép, nó sẽ tiến hành phá hoại. Loại này thường nguy hiểm vì chúng chỉ phá hoại một lần.

Loại liên tục: Sau khi bị lây nhiễm và liên tục, virus tiến hành phá hoại, song do tính liên tục này, các hoạt động phá hoại của nó không mang tính nghiêm trọng, chủ yếu là đùa cho vui.

2.2 F-virus

2.2.1 Kỹ thuật lây lan

Thêm vào đầu file.

Thông thường, phương pháp này chỉ áp dụng cho các file .COM, tức là đầu vào của chương trình luôn luôn tại PSP0h. Lợi dụng đầu vào cố định, virus chèn đoạn mã của chương trình virus vào đầu chương trình đối tượng, đẩy toàn bộ chương trình đối tượng xuống phía dưới. Cách này có một nhược điểm là do đầu vào cố định của chương trình.COM là PSP0, cho nên trước khi trả lại quyền điều khiển cho chương trình, phải đẩy lại toàn bộ chương trình lên bắt đầu từ offset 100h. Cách lây này gây khó khăn cho những người khôi phục vì phải đọc toàn bộ file vào vùng nhớ rồi mới tiến hành ghi lại.

Thêm vào cuối file.

Khác với cách lây lan ở trên, trong phương pháp này, đoạn mã của virus sẽ

được gắn vào sau của chương trình đối tượng. Phương pháp này được thấy trên hầu hết các loại virus vì phạm vi lây lan của nó rộng rãi hơn phương pháp trên.

2.2.2 Kỹ thuật đảm bảo tính tồn tại duy nhất

Trong vùng nhớ, thông thường các F-virus sử dụng hai kỹ thuật chính: Thứ nhất là tạo thêm chức năng cho DOS, bông cách sử dụng một chức năng con nào đó trong đó đặt chức năng lớn hơn chức năng cao nhất mà DOS có. Để kiểm tra chỉ cần gọi chức năng này, giá trị trả lại trong thanh ghi quyết định sự tồn tại của virus trong bộ nhớ hay chưa. Cách thứ hai là so sánh một đoạn mã trong vùng nhớ ấn định với đoạn mã của virus, nếu có sự chênh lệch thì có nghĩa là virus chưa có mặt trong vùng nhớ và sẽ tiến hành lây lan.

Trên file, có thể có các cách kiểm tra như kiểm tra bông test logic nào đó với các thông tin của Entry trong thư mục của file này. Cách này không đảm bảo tính chính xác tuyệt đối song nếu thiết kế tốt thì khả năng trùng lặp cũng hạn chế, hầu như không có, ngoài ra một ưu điểm là tốc độ thực hiện kiểm tra rất nhanh. Ngoài ra có thể kiểm tra bông cách dò một đoạn mã đặc trưng (key value) của virus tại vị trí ấn định nào đó trên file, ví dụ trên các byte cuối cùng của file.

2.2.3 Kỹ thuật thường trú

Đây là một kỹ thuật khó khăn, lý do là DOS chỉ cung cấp chức năng thường trú cho chương trình, nghĩa là chỉ cho phép cả chương trình thường trú. Vì vậy nếu sử dụng chức năng của DOS, chương trình virus muốn thường trú thì cả file đối tượng cũng phải thường trú, mà điều này thì không thể được nếu kích thước của file đối tượng quá lớn.

Chính vì lý do trên, hầu hết các chương trình virus muốn thường trú đều phải thao tác qua mặt DOS trên chuỗi MCB bằng phương pháp "thủ công". Căn cứ vào việc thường trú được thực hiện trước hay sau khi chương trình đối tượng thi hành, có thể chia kỹ thuật thường trú thành hai nhóm:

+ Thường trú trước khi trả quyền điều khiển.
+ Thường trú sau khi đoạt lại quyền điều khiển.

3. Ngăn chặn sự xâm nhập virus

Mục tiêu: Phòng ngừa được sự xâm nhập của virus

3.1 Sử dụng phần mềm diệt virus

Bảo vệ bằng cách trang bị thêm một phần mềm diệt virus có khả năng nhận biết nhiều loại virus máy tính và liên tục cập nhật dữ liệu để phần mềm đó luôn nhận biết được các virus mới.

Trên thị trường hiện có rất nhiều phần mềm diệt virus.Trong nước (Việt Nam): Bkav, CMC.Của nước ngoài: Avira, Kaspersky, AVG, ESET.Và phát hành bởi Microsoft: Microsoft Security Essentials

3.2 Sử dụng tường lửa

3.2.1 Sử dụng tường lửa bằng phần cứng

Nếu người sử dụng kết nối với mạng Internet thông qua một modem có chức năng này. Thông thường ở chế độ mặc định của nhà sản xuất thì chức năng "tường lửa" bị tắt, người sử dụng có thể truy cập vào modem để cho phép hiệu lực (bật). Sử dụng tường lửa bằng phần cứng không phải tuyệt đối an toàn bởi chúng thường chỉ ngăn chặn kết nối đến trái phép, do đó kết hợp sử dụng tường lửa bằng các phần mềm.

3.2.2 Sử dụng tường lửa bằng phần mềm

Ngay các hệ điều hành họ Windows ngày nay đã được tích hợp sẵn tính năng tường lửa bằng phần mềm, tuy nhiên thông thường các phần mềm của hãng thứ ba có thể làm việc tốt hơn và tích hợp nhiều công cụ hơn so với tường lửa phần mềm sẵn có của Windows.

3.3 Cập nhật các bản sửa lỗi của hệ điều hành

Hệ điều hành Windows (chiếm đa số) luôn luôn bị phát hiện các lỗi bảo mật chính bởi sự thông dụng của nó, tin tặc có thể lợi dụng các lỗi bảo mật để chiếm quyền điều khiển hoặc phát tán virus và các phần mềm độc hại

3.4 Vận dụng kinh nghiệm sử dụng máy tính

Cho dù sử dụng tất cả các phần mềm và phương thức trên nhưng máy tính vẫn có khả năng bị lây nhiễm virus và các phần mềm độc hại bởi mẫu virus mới chưa được cập nhật kịp thời đối với phần mềm diệt virus. Người sử dụng máy tính cần sử dụng triệt để các chức năng, ứng dụng sẵn có trong hệ điều hành và các kinh nghiệm khác để bảo vệ cho hệ điều hành và dữ liệu của mình

3.5 Bảo vệ dữ liệu máy tính

Nếu như không chắc chắn 100% rằng có thể không bị lây nhiễm virus máy tính và các phần mềm hiểm độc khác thì bạn nên tự bảo vệ sự toàn vẹn của dữ liệu của mình trước khi dữ liệu bị hư hỏng do virus (hoặc ngay cả các nguy cơ tiềm tàng khác như sự hư hỏng của các thiết bị lưu trữ dữ liệu của máy tính).

3.6 Sao lưu dữ liệu theo chu kỳ

Là biện pháp đúng đắn nhất hiện nay để bảo vệ dữ liệu. Bạn có thể thường xuyên sao lưu dữ liệu theo chu kỳ đến một nơi an toàn như: các thiết bị nhớ mở rộng (ổ USB, ổ cứng di động, ghi ra đĩa quang...), hình thức này có thể thực hiện theo chu kỳ hàng tuần hoặc khác hơn tuỳ theo mức độ cập nhật, thay đổi của dữ liệu của bạn.

3.7 Tạo các dữ liệu phục hồi cho toàn hệ thống

Không dừng lại các tiện ích sẵn có của hệ điều hành (ví dụ System Restore của Windows Me, XP...) mà có thể cần đến các phần mềm của hãng thứ ba, ví dụ bạn có thể tạo các bản sao lưu hệ thống bằng các phần mềm ghost, các phần mềm tạo ảnh ổ đĩa hoặc phân vùng khác.

Thực chất các hành động trên không chắc chắn là các dữ liệu được sao lưu không bị lây nhiễm virus, nhưng nếu có virus thì các phiên bản cập nhật mới hơn của phần mềm diệt virus trong tương lai có thể loại bỏ được chúng.

4- Bài tập thực hành

Bài tập 1: Cách cài đặt Windows Security Essentials cho Windows Server 2012 R2

Yêu cầu: Cài đặt và chạy chương trình diệt virus

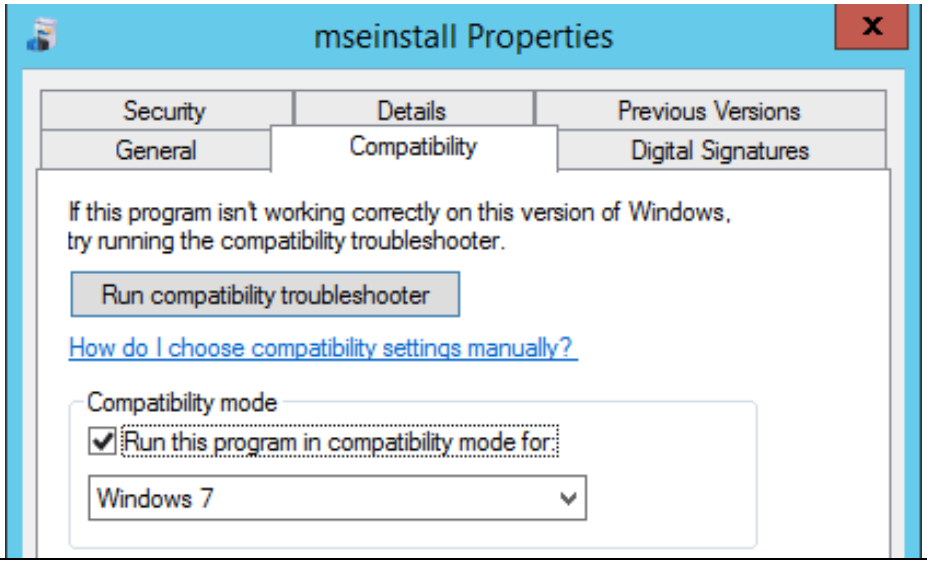
Chuẩn bị: http://windows.microsoft.com/en-us/windows/security-essentials-all-versions

Thực hiện

Bước 1: Để tránh lỗi này, vào thư mục chứa file mseinstall.exe →*Properties*.

Microsoft Security Essentials
Microsoft Security Essentials installation error
Microsoft Security Essentials
Microsoft Security Essentials cannot be installed on your operating system
Your version of the Windows operating system is not supported by this program.
For information about supported operating systems, see the online Help.

Bước 2: Tab Compatibility→Compatibility Mode →Windows 7→OK.

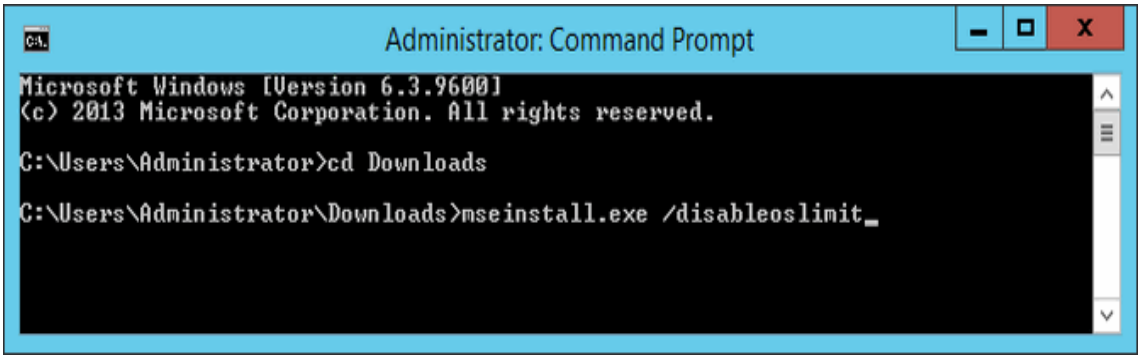


Bước 3: double click vào file để cài đặt, sẽ lại gặp thông báo lỗi như bên dưới này

Microsoft Security Essentials
Microsoft Security Essentials installation error
Microsoft Security Essentials
Microsoft Security Essentials cannot be installed on your operating system
Your version of the Windows operating system is not supported by this program.
For information about supported operating systems, see the online Help.

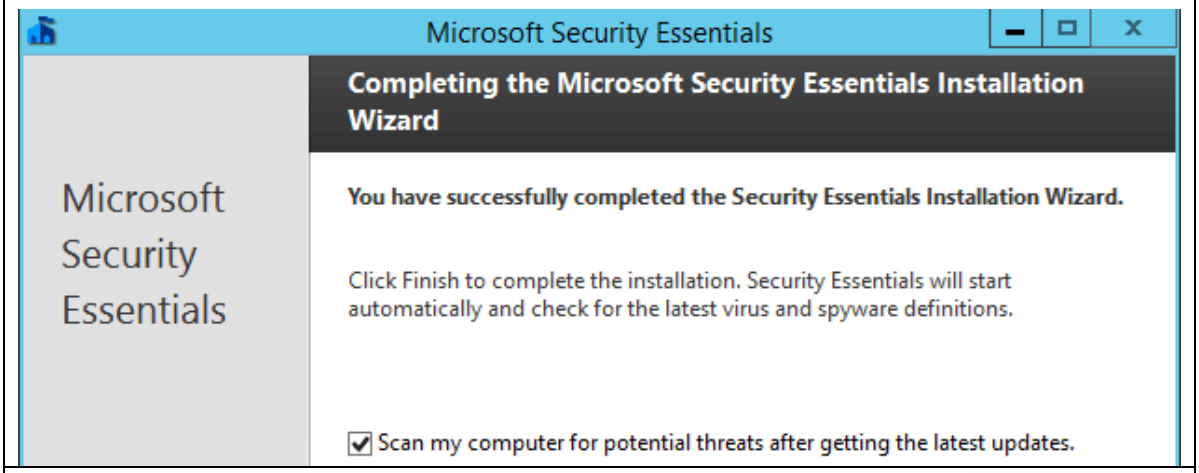
Bước 4: file mseinstall.exe→bấm giữ phím Shift→click phải chuột. "*Open command windows here*"

nhập vào dòng lệnh sau: *mseinstall.exe file with the /disableoslimit*



Tiến hành cài đặt

Bước 5: Finish → "*Scan my computer for potential threats after getting the latest updates*" →Finish.

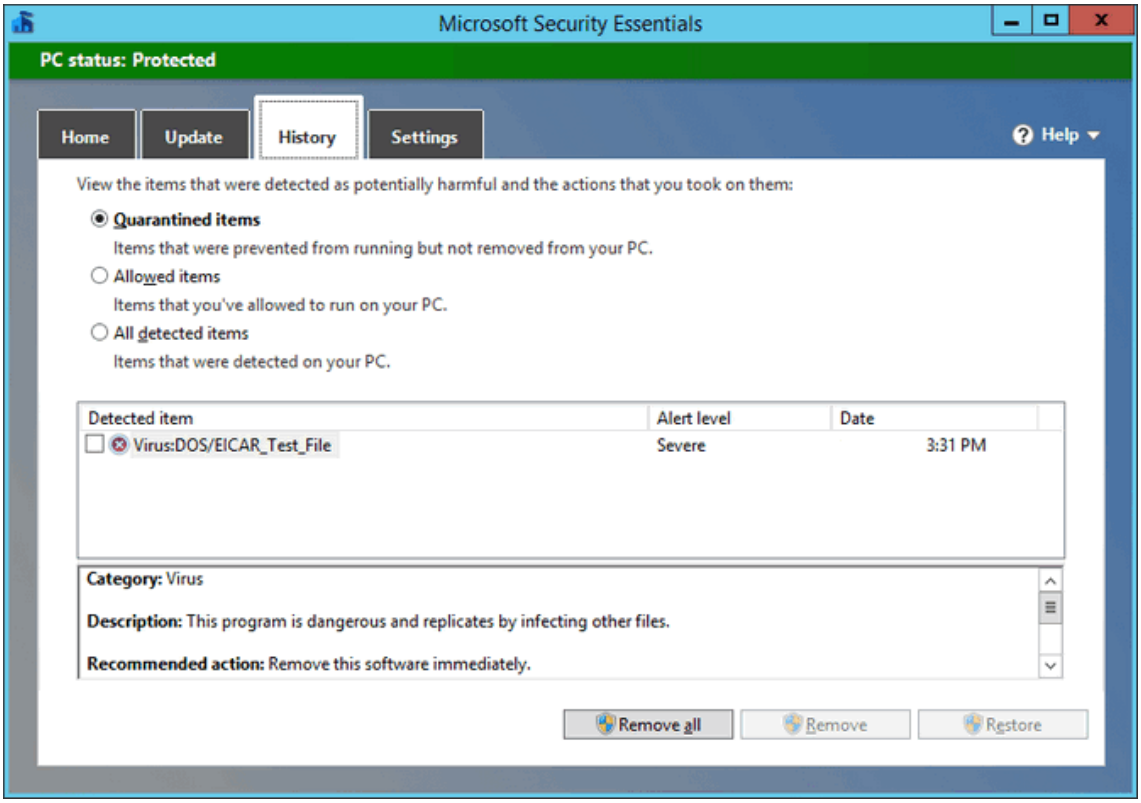

Microsoft Security Essentials
Completing the Microsoft Security Essentials Installation Wizard
Microsoft Security Essentials
You have successfully completed the Security Essentials Installation Wizard.
Click Finish to complete the installation. Security Essentials will start automatically and check for the latest virus and spyware definitions.
Scan my computer for potential threats after getting the latest updates.

Bước 6: truy cập https://www.eicar.org/86-0-Intended-use.html

copy đoạn mã :X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-

ANTIVIRUS-TEST-FILE!$H+H* → Hãy dán đoạn mã trên vào notepad

Chạy chương trình



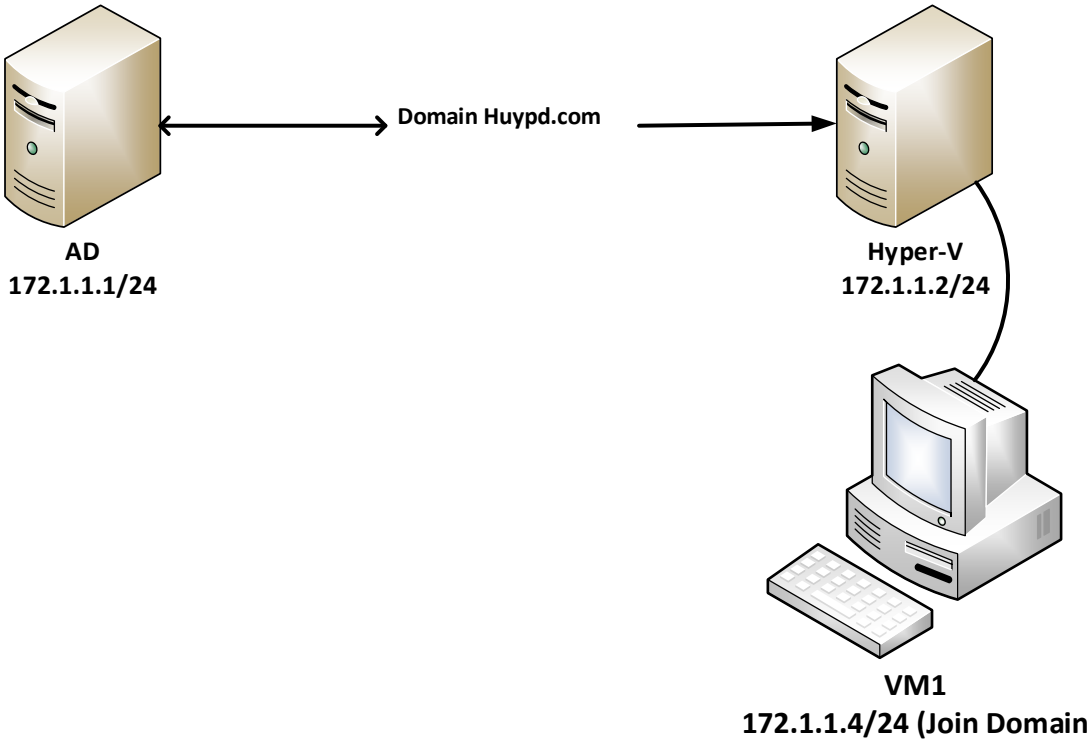
Nếu mở Windows Security Essentials lên, click vào tab History, sẽ thấy tập tin nằm trong mục Quarantined Items và có tên của con "virus" dùng để thử nghiệm trong phần Detected item

Bài tập 2 : Cross Live Migration cho phép di dời các máy ảo từ Hyper-V chạy nền tảng Windows Server 2012 sang Windows Server 2012 R2. Đồng thời cũng hỗ trợ cho phép chuyển đổi các máy ảo thế hệ 1 từ Hyper-V host Windows Server 2008 sang Hyper-V host Windows Server 2012 R2 để chạy. Như vậy, Hyper-V 2012 R2 cho phép chạy cả 2 loại thế hệ máy ảo. Chống lại virus xâm nhập hệ thống

Yêu cầu: Tạo máy ảo thế hệ 2 trên Windows Server 2012 R2 →chống lại virus xâm nhập hệ thống

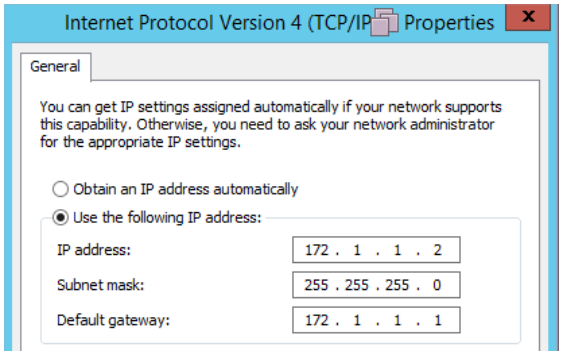
Chuẩn bị

- 1 máy win 2012 → DC
- 1 máy win 2012→ Hyper-V
- 1 máy win 8



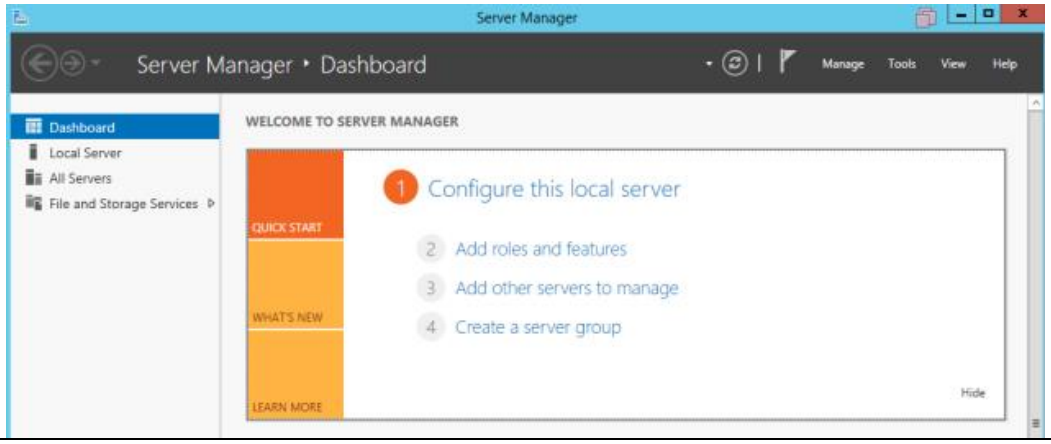
Thực hiện

Bước 1: Cấu hình địa chỉ IP và join domain vào máy AD

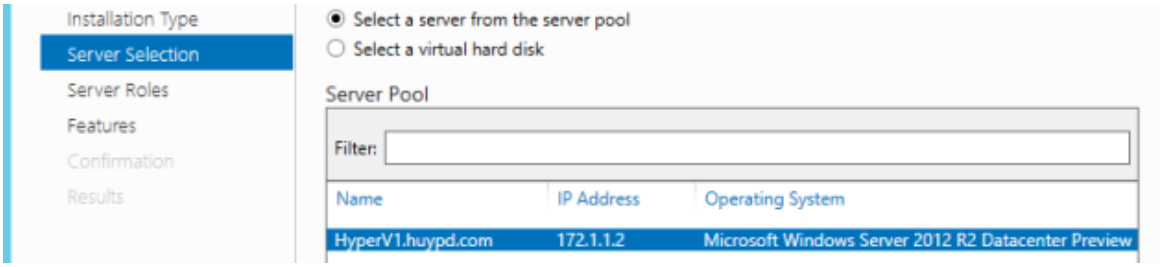

Internet Protocol Version 4 (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 172 . 1 . 1 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 172 . 1 . 1 . 1

tiến hành join vào →AD

Bước 2: Cài tính năng Hyper-V cho máy vật lý Hyper-V1→Server Manager →Add roles and features

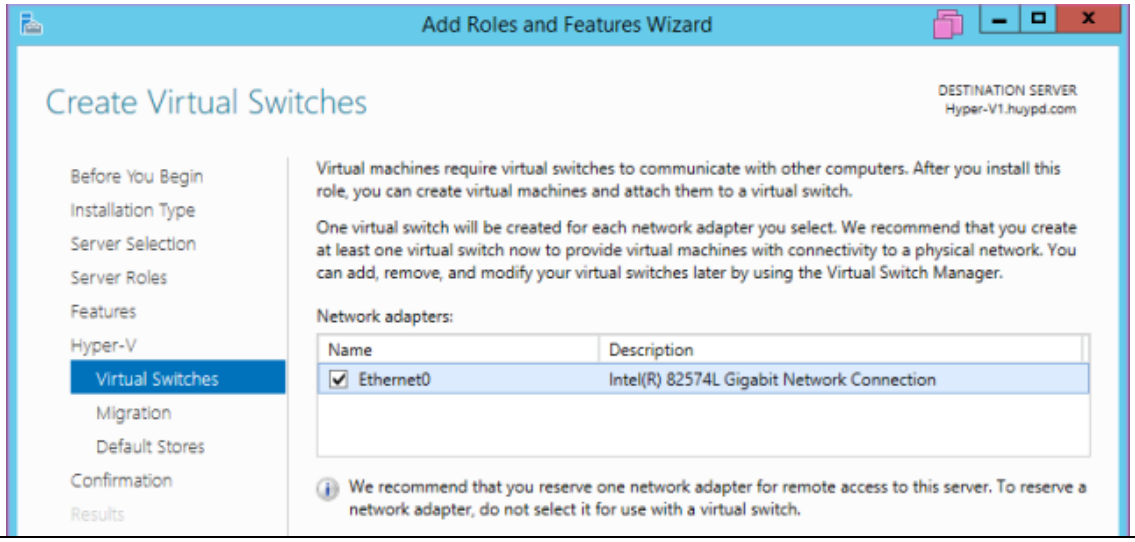


Bước 3: Server selection →Hyper huypd.com→Next

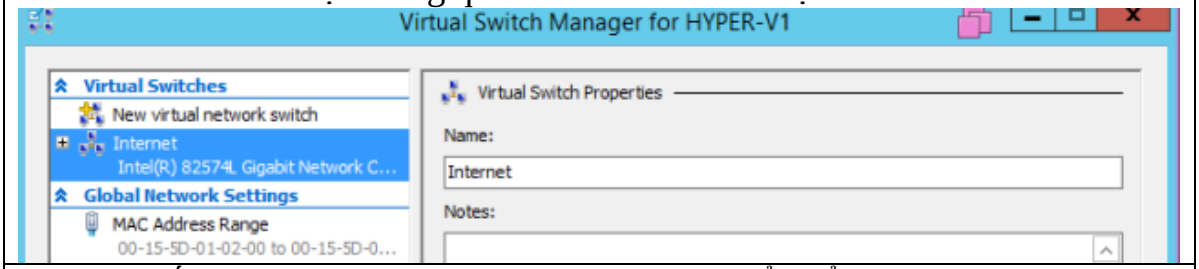


Chọn Hyper→Next

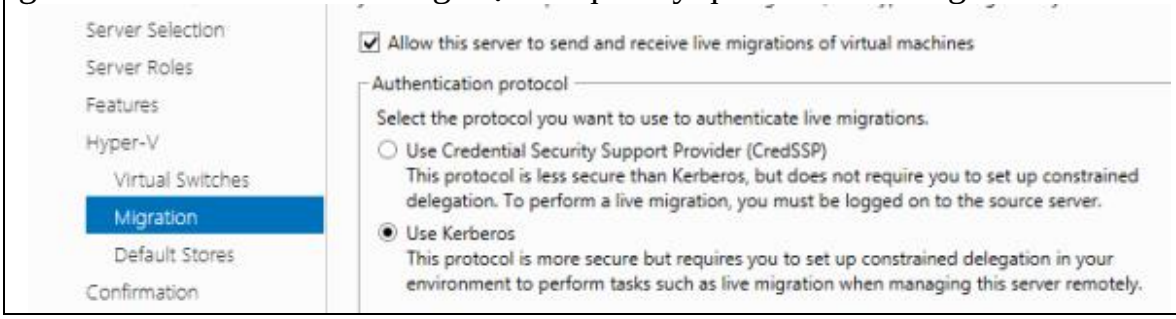
Bước 4: Về phần Network (Adapter Network) của máy ảo được quản lý bởi Virtual Switches, bước này cho phép chúng ta khai báo card mạng vật lý của máy Hyper-V host vào Virtual Switches để các máy ảo có thể dùng card này giao tiếp được với bên ngoài.


Add Roles and Features Wizard
Create Virtual Switches
DESTINATION SERVER
Hyper-V1.huypd.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Hyper-V
Virtual Switches
Migration
Default Stores
Confirmation
Results
Virtual machines require virtual switches to communicate with other computers. After you install this role, you can create virtual machines and attach them to a virtual switch.
One virtual switch will be created for each network adapter you select. We recommend that you create at least one virtual switch now to provide virtual machines with connectivity to a physical network. You can add, remove, and modify your virtual switches later by using the Virtual Switch Manager.
Network adapters:
Name
Description
Ethernet0
Intel(R) 82574L Gigabit Network Connection
We recommend that you reserve one network adapter for remote access to this server. To reserve a network adapter, do not select it for use with a virtual switch.

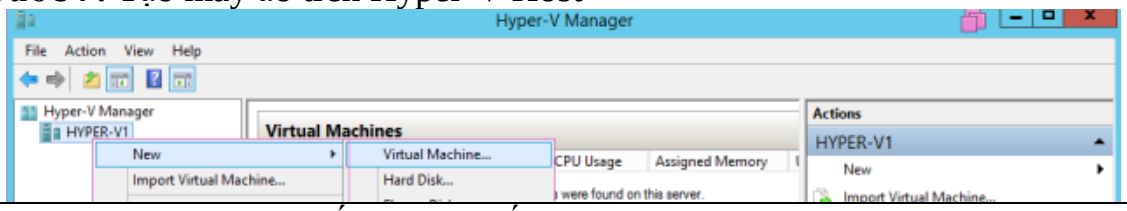
Bước 5: Chuột phải Hyper-V1 → Chọn Virtual Switch Manager → Chọn Virtual Switch vừa tạo trong quá trình cài Role → đặt Name là : "Internet"



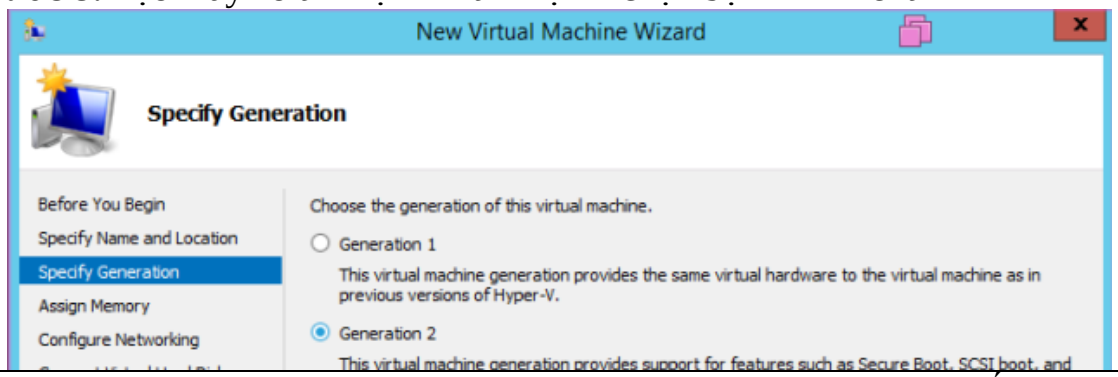
Bước 6: cấu hình tính năng Live Migration (chuyển đổi máy ảo từ Hyper-V host vật lý này sang Hyper-V host khác trong Domain). Thường thì sử dụng giao thức Kerberos để chứng thực và quản lý quá trình live migration.


Server Selection
Server Roles
Features
Hyper-V
Virtual Switches
Migration
Default Stores
Confirmation
Allow this server to send and receive live migrations of virtual machines
Authentication protocol
Select the protocol you want to use to authenticate live migrations.
Use Credential Security Support Provider (CredSSP)
This protocol is less secure than Kerberos, but does not require you to set up constrained delegation. To perform a live migration, you must be logged on to the source server.
Use Kerberos
This protocol is more secure but requires you to set up constrained delegation in your environment to perform tasks such as live migration when managing this server remotely.

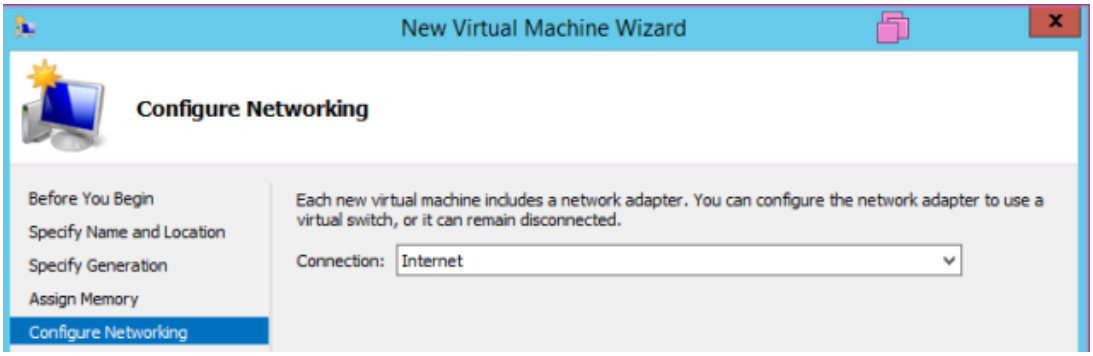
Bước 7: Tạo máy ảo trên Hyper-V Host



Bước 8: Tạo máy ảo thế hệ 1 → thế hệ 2→chọn bộ nhớ→Next

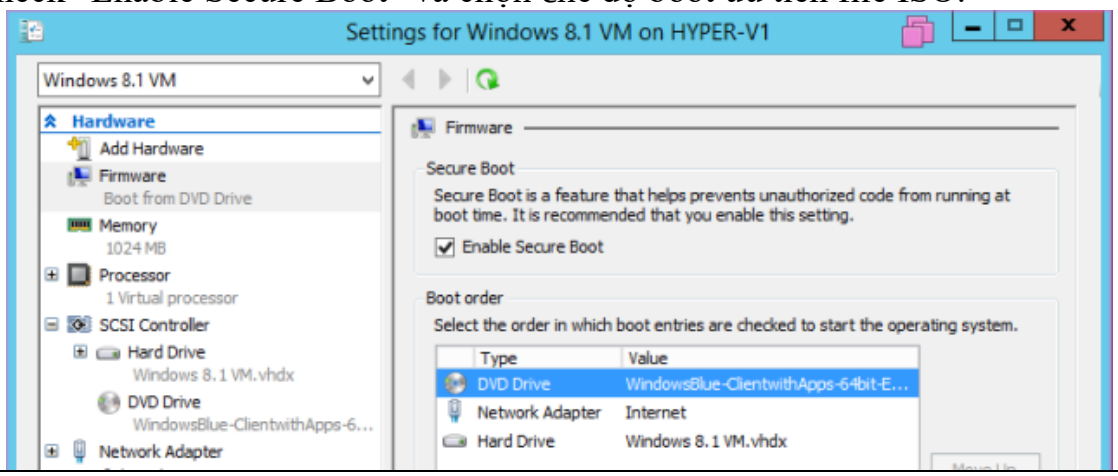

New Virtual Machine Wizard
Specify Generation
Before You Begin
Specify Name and Location
Specify Generation
Assign Memory
Configure Networking
Choose the generation of this virtual machine.
Generation 1
This virtual machine generation provides the same virtual hardware to the virtual machine as in previous versions of Hyper-V.
Generation 2

Bước 9: Khai báo Network trong Virtual Switches cho máy ảo→ Cấu hình dung lượng file VHD của máy ảo và vị trí lưu máy ảo trong Hyper-V Host→Next

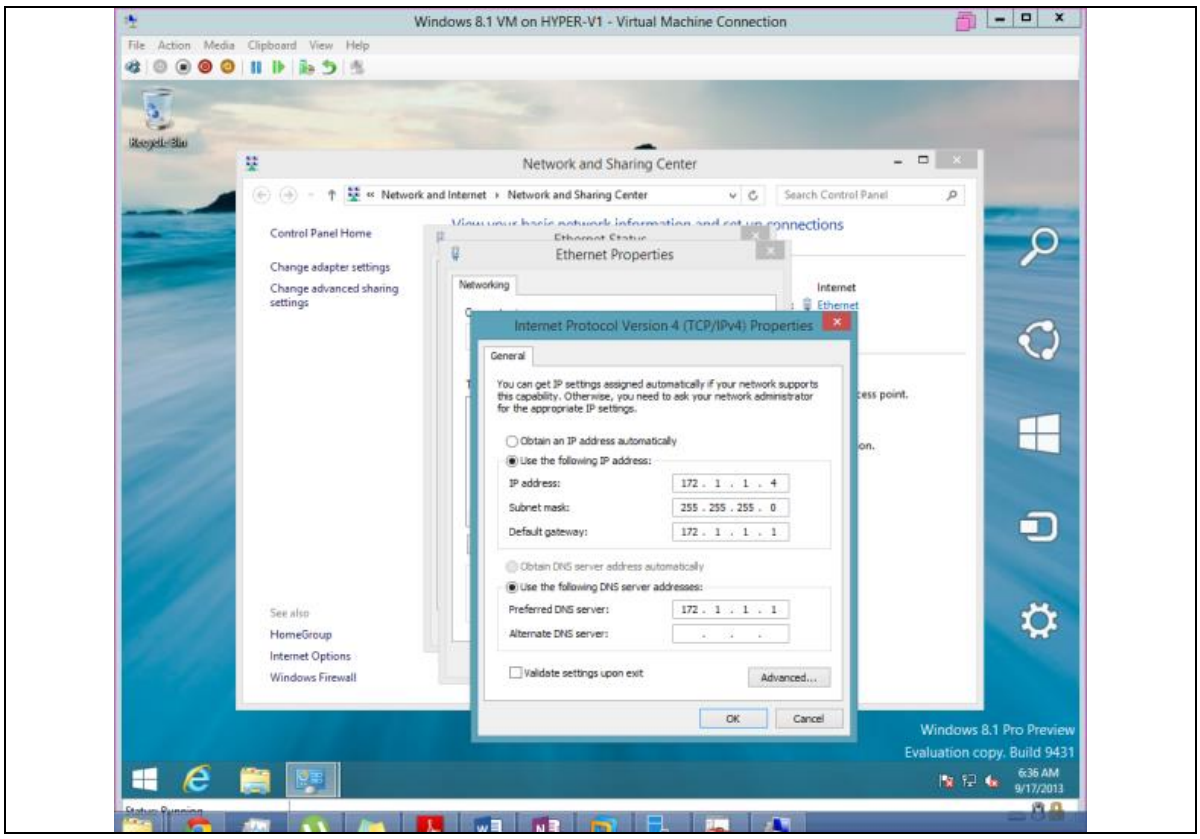

New Virtual Machine Wizard
Configure Networking
Before You Begin
Specify Name and Location
Specify Generation
Assign Memory
Configure Networking
Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.
Connection:
Internet

chọn file cài đặt

Bước 11: Chuột phải máy ảo vừa tạo và chọn Settings → FirmWare → bỏ check "Enable Secure Boot" và chọn chế độ boot ưu tiên file ISO.



Bước 12: khởi động máy ảo lên→ Nhập CD-Key→ Join domain cho máy ảo vào Domain : Huypd.com và đặt địa chỉ IP.


Windows 8.1 VM on HYPER-V1 - Virtual Machine Connection
Network and Sharing Center
Ethernet Properties
Internet Protocol Version 4 (TCP/IPv4) Properties
Windows 8.1 Pro Preview
Evaluation copy. Build 9431

5-TÓM TẮT NỘI DUNG

- Virus lây nhiễm theo cách cổ điển
- Virus lây nhiễm qua thư điện tử
- Lây nhiễm vào các file đính kèm
- Lây nhiễm do mở một liên kết trong thư điện tử
- Lây nhiễm ngay khi mở để xem thư điện tử
- Virus lây nhiễm qua mạng Internet
- Virus có khả năng vô hiệu hoá phần mềm diệt virus
- Cách phòng chống virus và ngăn chặn tác hại của nó
- Sử dụng phần mềm diệt virus
- Sử dụng tường lửa
- Cập nhật các bản sửa lỗi của hệ điều hành
- Vận dụng kinh nghiệm sử dụng máy tính

6- CÂU HỎI VÀ BÀI TẬP

CÂU HỎI

Câu 1: Trình bày về virus máy tính và các chương trình mã độc:Khái niệm, phân loại các chương trình mã độc. Phân biệt virus, sâu (worm), zombie. Trình bày cấu trúc chung của một virus, kỹ thuật tránh phát hiện bằng việc nén chương trình chủ. Các loại virus (file virus, virus boot sector,

virus đa hình, virus macro). Kỹ thuật giải mã họ virus để phát hiện và diệt các virus đa hình.

Câu 2: Liệt kê và phân loại các phần mềm có hại và các biện pháp phòng chống

Câu 3: Trình bày công dụng của 10 phần mềm diệt virus hiện nay do trung tâm an ninh mạng xếp hạng.

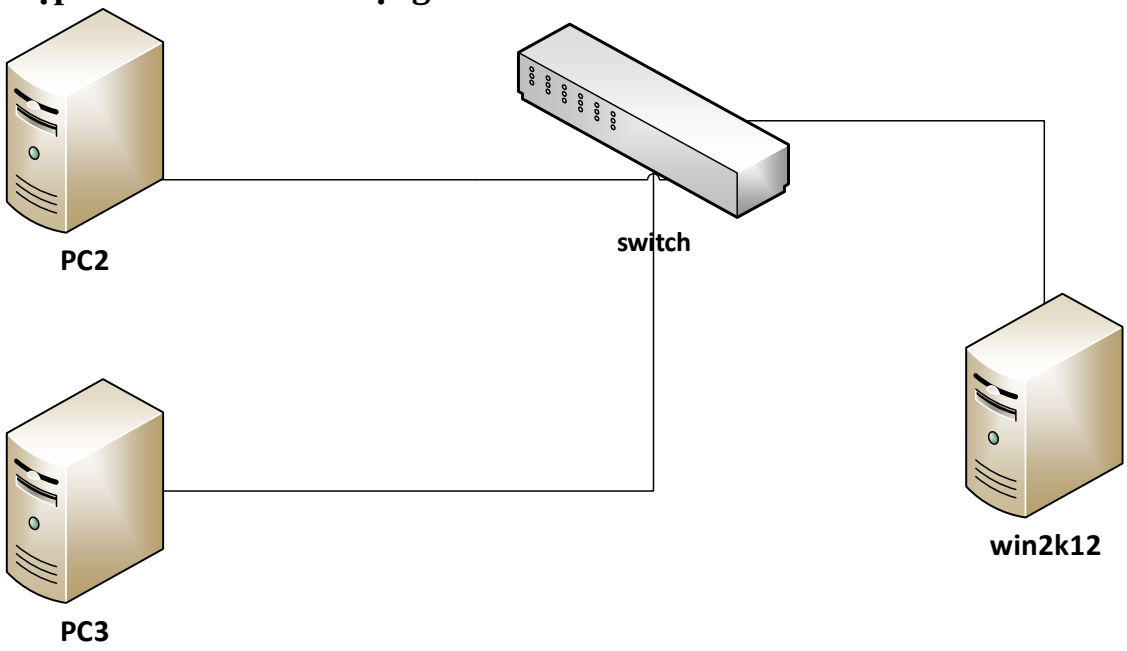
Câu 4: Phân tích các kỹ thuật xâm nhập hệ thống và cách phòng ngừa.

Câu 5: Nêu các biện pháp tăng cường an ninh, bảo mật máy tính cá nhân dựa trên các phần mềm thông dụng hiện có.

Câu 6: Chọn và triển phần mềm quản lý, giám sát kết nối mạng tốt nhất

BÀI TẬP

Bài tập 1: Cho mô hình mạng



Yêu cầu: Người dùng máy tính tại Việt Nam khá quen thuộc với phần mềm diệt virus Norton của hãng bảo mật danh tiếng Symantec. Tuy nhiên, các dòng sản phẩm norton như Norton 360, Norton Internet Security, Norton Antivirus không cài được trên máy chủ (server).

Cài đặt, cấu hình phần mềm diệt virus Symantec Endpoint Protection Small Business Edition 12.1 dùng cho 1 máy chủ

Chuẩn bị:

- Cả 3 máy tắt Firewall
- PC2 & PC3 Join Domain
- Máy đóng vai trò SEP Manager add roles services Web Server (IIS)
    - ASP.net
    - CGI
    - IIS6 Management compatibility
- Kiểm tra Computer Browser services Start

Hướng dẫn làm bài

1.Cài đặt Symantec Endpoint Protection:

B1: Click Install SymantecEndpoint ProtectionManager → Next→ Accept→ Next→ Cửa sổ Select Web Site : Create a custom Web site (recommended) → Finish

B2: Chọn Database Type : Simple → Khai báo thông tin→ Cửa sổ Data Colletion → Next → Next

B3: Quá trình tạo Database → Hiện lên hộp thoại Deployment Wizard → Yes → Finish

2.Tạo Package để Deploy cho Client

B1: Cửa sổ Migration and Deployment Wizard → Next→ Deploy the Windows client → Next

B2: Đặt tên Group : SEPClient → Next→ Option cho package → Next

B3: Chỉ ra nơi lưu trữ Package (C:Deploy) → Next→ No, just create them and I'll deploy them later → Finish

3.Cấu hình Symantec Endpoint Protection tích hợp vào Active Directory

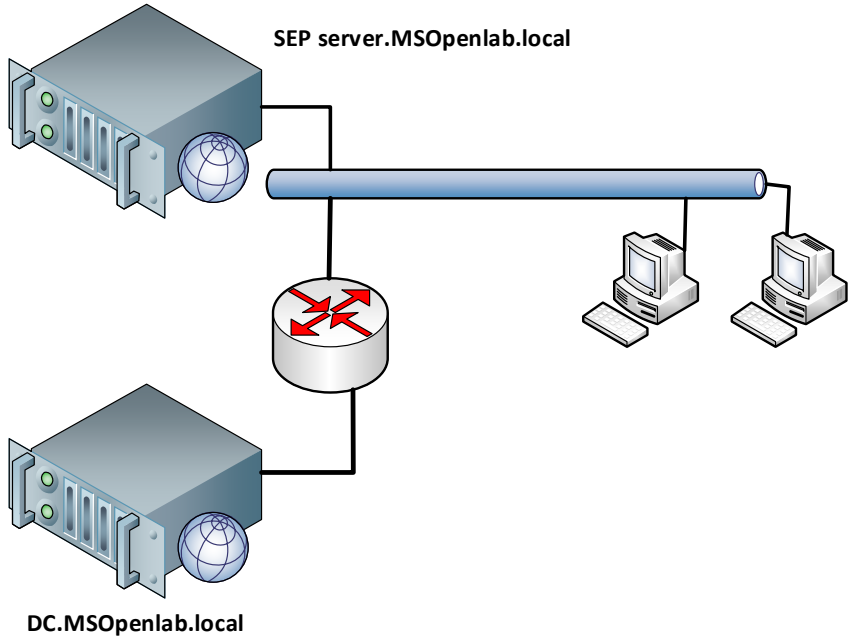
B1: Khai báo Acitve Directory or LDAP Server:→ Cửa sổ SEP Manager Console → Logon với quyền Admin (Môi trường chỉ có 1 Domain thì dòng Domain để trắng → Logon Default Domain)

B2: SEPManager console → Admin → Click SEPM → Edit Properties→ Tab Directory Server → Add

B3: Import Organizational Unit or Container từ Active Directory→ SEP Manager Console -> Clients → Tasks → Import Organizational Unit or Container → Select Domain

B4: **Chọn OU hoặc Container cần Import → OK→ Kiểm tra trong cột View Client xuất hiện nội dung vừa Import**

Bài tập 2: Cho mô hình mạng



Yêu cầu:

- Cài đặt Symantec Endpoint Protection Manager 11.0.6
- Triển khai cài đặt từ xa cho client.

Chuẩn bị:

- 1 PC Windows Server 2008 R2 : Domain Controller.
- 1 PC Windows Server 2008 R2: Symantec Endpoint Server (dùng cài đặt Sysmatec Endpoint Protection Manager).
- 1 PC Windows 7 : Symantec Endpoint Client.
- Các máy tính đã join domain, tắt windows firewall.

Hướng dẫn làm bài

1. Cài đặt Sysmatec Endpoint Protection 11.0.6

B1: Mở source → file Setup.exe→Symantec Endpoint Protection Installation Program→ Install Symatec Endpoint Protection Manager.

B2: Wellcome to the Install Wizard for Symantec Endpoint Protection Manager→ Next→License Agreement, chọn I accept the term in the license agreement→ Next.

B3: Destination Folder→Next→Select Web Site, chọn cấu hình mặc định. →Next→Ready to Install the Program→ Install→Finish

B4: Welcome to the Management Server Configuration Wizard→Advanced. →Next→Approximately how many computer… →Between 100 and 500. →Next.

B5: **What would you like to do→ Install my first site→Next.**

B6: **Specify the server name… → Next→What do you want to name this site →Next.**

B7: The management server and client computer… Nhập thông tin vào 2 khung Create encryption password và Confirm encryption password→ Next→Next→Next→Next→Finish.

2. Triển khai cài đặt từ xa cho client

B1: Start→All Programs→Migration and Deployment Wizard→Welcome to the Migration and Deployment Wizard→Next→Next

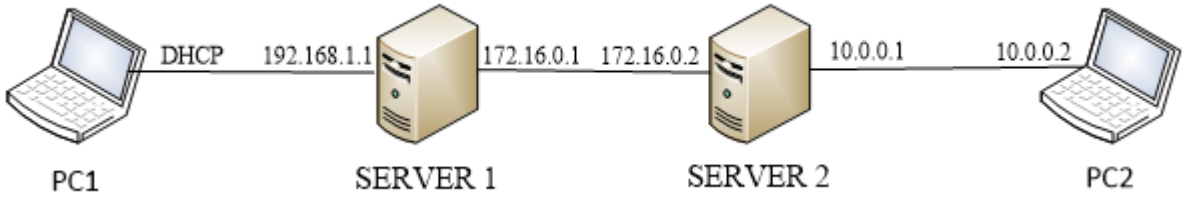
B2: Chọn 32-bit Client Install Package→Browse.. →OK→ Next→ Finish

B3: Chọn vào client→ Add→ OK→ Next→ Finish→ Yes

B4: Kiểm tra trên client đã được cài đặt Symantec Endpoint→ Trên máy client chọn Restart Now để cập nhật đầy đủ thông tin từ server

B5: Mở Symantec Endpoint Protection Manager Console,chọn vào Clients, chọn vào MSOpenlab_siteA. Kiểm tra đã có client vừa cài đặt.

Bài tập 3: Cho mô hình



Yêu cầu:

Câu 1:

a) Nâng cấp Server1 thành domain controller với tên domain là cdnqtm.edu.vn.

b) Cài đặt và cấu hình dịch vụ DHCP trên Server1 sao cho:

- Mạng LAN 1 nhận địa chỉ IP trong khoảng từ 192.168.1.10 đến 192.168.1.100, địa chỉ default gateway và DNS.
- Mạng LAN 3 nhận địa chỉ IP trong khoảng từ 10.0.0.10 đến 10.0.0.100, địa chỉ default gateway và DNS.

Câu 2:

a) Cài đặt và cấu hình dịch vụ RAS (Remote Access Service) để PC01 ping được PC02.

b) Nâng cấp Server2 thành backup domain controller và DNS server cho Server1.

c) Gia nhập PC01 vào domain cdnqtm.edu.vn.

Câu 3:

a) Thực hiện các chính sách hệ thống sau:

- Quy định số lần cố gắng đăng nhập trước khi tài khoản bị khóa là 3.
- Quy định thời gian khóa tài khoản nếu đăng nhập quá số lần cho phép là 45 phút.

b) Tạo 3 domain user là sinhvien1, sinhvien2, sinhvien3 sao cho:

- Dùng shadow copy để phục hồi dữ liệu trên C:\DATA của máy Server1 cho sinhvien1.

Câu 4 :

Sử dụng thêm 2 physcial disk trên Server1, mỗi đĩa có dung lượng 100MB. Sau đó tạo thêm các volume sau:

- Spanned volume kích thước: (10MB, 20MB).
- Mirror volume kích thước: (40MB, 40 MB).

Chuẩn bị:

- 2 máy PC cài đặt win2k8
- 2 máy PC cài đặt win7
- 2 sợi cáp thẳng
- 2 sợi cáp chéo
- 1 switch
- Thiết lập địa chỉ IP
- Đấu nối theo mô hình

Hướng dẫn làm bài

Câu 1:

a.Nâng cấp Server1 thành domain controller với tên domain là cdnqtm.edu.vn.

b.Cài đặt và cấu hình dịch vụ DHCP trên Server1

B1: Server Manager → Add Roles → DHCP Server →Next**.**

B2: Chọn địa chỉ mạng LAN 1 → **Next.**

B3: Nhập tên Domain Name, DNS Server → Nex

B4: Chọn Disable DHCPv6… →Next.

B5: Install → Close.

B6: Server Manager → DHCP Server → R-Click Server Name → All Tasks →Restart.

B7: CMD → gõ lệnh ipconfig /renew để kiểm tra DHCP và xin ip cho PC1

Câu 2 :

a.Cài đặt và cấu hình dịch vụ RAS (Remote Access Service) để PC01 ping được PC02

B1: Start → Administrative Tools → Routing and Remote Access → Ipv4 → Static Routes → New Static Rout…

B2: R-Click server → All Task → Restart.

B3: Thực hiện tương tự trên server 2

b.Nâng cấp Server2 thành backup domain controller và DNS server cho Server1

B1:Trên Server 2: Server Manager → Add Roles → Active Directory Domain Services → Next → Install.

B2: Nhập tên Domain → Next → Đăng nhập bằng tài khoản và password của Administrator Domain

B3: Chọn DNS, Global catalog →Next.

B4: Đặt Password khôi phục → Next

B5: Tích chọn Reboot on completion → Chờ khởi động lại là xong

CÁC THUẬT NGỮ CHUYÊN MÔN

Các từ viết tắt	Tên đầy đủ	Ý nghĩa
AD	Active Directory	Dịch vụ thư mục
BDC	Backup Domain Controller	Sao lưu domain
DC	Domain Controller	Bộ điều khiển miền
DNS	Domain Name System	Hệ thống tên miền
IP	Internet Protocol	Giao thức Internet
OU	Oranization Unit	Đơn vị tổ chức
PDC	Primary Domain Controller	Bộ điều khiển tên miền chính
TCP	Transmission Control Protocol	Giao thức điều khiển truyền tin
W2K3	Windows server 2003	Hệ điều hành windows server 2003
W2K8	Windows server 2008	Hệ điều hành windows server 2008
WXP	Windows XP	Hệ điều hành windows XP
Win7	Windows 7	Hệ điều hành windows7
FQDN	Full Qualified Domain Name	Tên miền đầy đủ được chứng nhận
HĐH	Hệ Điều Hành	Hệ Điều Hành
CSDL	Cơ Sở Dữ Liệu	Cơ Sở Dữ Liệu
MSDE	Microsoft Database Engine	Công nghệ cơ sở dữ liệu
RUP	Roaming User Profile	Cho phép Profile lưu trên server kèm theo user

PAP	Password Authentication Protocol	Giao thức xác nhận mật mã
CHAP	Challenge Handshake Authentication Protocol	Giao thức bảo mật dựng sẵn
EAP	Extensible Authentication Protocol	Phương thức bảo mật cho mạng không dây
DFS	Distributed File System	Hệ thống bảo mật
NAT	Network Address Translation	Biên dịch địa chỉ mạng
IPSec	Internet Protocol SECurity	Giao thức xác thực và mã hóa IP
SQL	Structured Query Language	Ngôn ngữ truy vấn
RRAS	Routing and Remote Access	Cấu hình định tuyến bằng giao diện
RDP	Remote Desktop Protocol	Tính năng truy cập máy tính trong mạng
EFS	Encrypting File System	Mã hóa dữ liệu
DFS	Distributed File System	Hệ thống tập tin phân tán
STMP	Simple Mail Transfer Protocol	Giao thức truyền thư đơn giản
SSH	Secure Shell	Dịch vụ truy cập từ xa
SSL	Secure Socket Layer	Tầng socket an toàn
RIP	Routing Information Protocol	Một kiểu giao thức dẫn đường
RARP	Reverse Address Resolution Protocol	Giao thức chuyển đổi từ địa chỉ vật lý sang địa chỉ IP
NIC	Network Interface Card	Card giao tiếp mạng
MAC	Media Access Control	Địa chỉ thiết bị
LAN	Local Area Network	Mạng nội bộ

IGMP	Internet Group Management Protocol	Giao thức Internet để các host kết nối, huỷ kết nối từ các nhóm multicast
HTTP	Hyper Text Transfer Protocol	Giao thức truyền siêu văn bản
FIB	Forwarding Information Table	Bảng thông tin chuyển đổi định tuyến
POP3	Post Office Protocol version 3	là một giao thức tầng ứng dụng, dùng để lấy thư điện tử từ server mail
NTFS	New Technology File System	Hệ thống tập tin công nghệ mới
SAM	Security Accounts Manager	Bảo mật tài khoản quản lý
SOA	Start of Authority	Thông tin về domain trên DNS Server
SID	Security Identifier	Định danh bảo mật
MMC	Microsoft Management Console	Công cụ quản lý và cấu hình windows
RR	Resource Record	Mẫu thông tin dùng để mô tả các thông tin về cơ sở dữ liệu DNS
FTP	File Transfer Protocol	Giao thức truyền file
URL	Uniform Resouce Locator	Địa chỉ tài nguyên thống nhất

TÀI LIỆU THAM KHẢO

- Tài liệu quản trị windows server 2003, tác giả Trung tâm tin học Đại học Khoa học Tự nhiên TPHCM, xuất bản năm 2003
- Các bài Lab MCSA, tác giả trung tâm đào tạo mạng máy tính Nhất Nghệ xuất bản năm 2005
- Tài liệu Windows Server 2003 tập 1,2,3, tác giả Phạm Hoàng Dũng do nhà xuất bản thống kê xuất bản năm 2005